(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－328269

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Ｚ
Ｇ０７Ｆ　7/08		Ｇ０７Ｇ　1/12	３２１Ｍ
Ｇ０７Ｇ　1/12	３２１	Ｇ０９Ｃ　1/00	６６０Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０７Ｆ　7/08	Ｍ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｃ

審査請求　未請求　請求項の数18　ＯＬ　（全 35 頁）

(21)出願番号　特願平10－133550

(22)出願日　平成10年(1998)５月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　梅澤　克之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

最終頁に続く

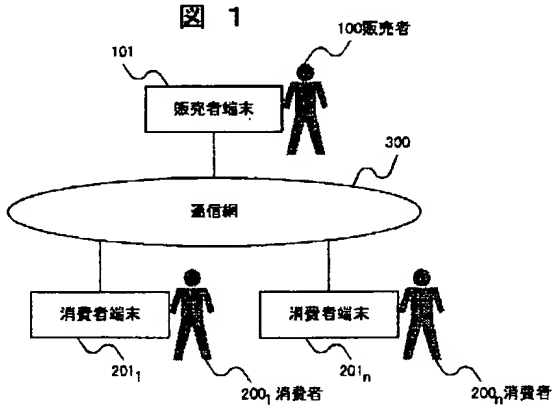
(54)【発明の名称】　電子クーポンシステムおよび電子クーポン発券・検証方法

(57)【要約】

【課題】電子的に発券されたクーポンを印刷して使用する場合でも、クーポンの偽造や改ざん，第三者によるクーポンの不正使用を検出することを可能とする。

【解決手段】クーポン発券時に、販売者１００は、消費者２００から送信されたパスワードの不可逆変換値と、改ざんされては困るクーポン情報と、クーポン情報のデジタル署名とを、印刷しても目視可能なデータとして記載したクーポンを作成するので、消費者２００がクーポンを印刷して使用する場合でも、クーポンに記載されているデジタル署名を検証することで、クーポンの改ざんや偽造を検出することができる。また、消費者２００は、クーポンの使用時に、発券時と同じパスワードを販売者１００に提示し、販売者１００は、提示されたパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較することで、第三者によるクーポンの不正使用を検出することができる。

図１



【特許請求の範囲】

【請求項１】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなり、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、

上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、

上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、

上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、

上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、

上記販売者端末のクーポン発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、

上記販売者端末のクーポン検証手段は、

上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、

該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、

上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、

印刷されたクーポンに記載されている不可逆変換値とクーポン情報と暗号化情報とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、取得した暗号化情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項２】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなり、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、

上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、

上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、

上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、

上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、

上記販売者端末のクーポン発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における販売者の秘密鍵を用いて暗号化したデジタル署名と、上記クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、

上記販売者端末のクーポン検証手段は、

上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、

該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、

上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、

印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得

られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項３】請求項１または２記載の電子クーポンシステムであって、

上記販売者端末のクーポン発券手段は、

作成したクーポンと共に、公開鍵暗号方式における販売者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信し、

上記消費者端末のクーポン受信手段は、

受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項４】請求項１，２または３記載の電子クーポンシステムであって、

上記クーポン情報は、クーポンごとに固有のシリアル番号を含み、

上記販売者端末は、

効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を記憶するシリアル番号記憶手段を備え、

上記販売者端末のクーポン検証手段は、

検証対象のクーポンに記載されているクーポン情報中のシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証することを特徴とする電子クーポンシステム。

【請求項５】請求項１，２，３または４記載の電子クーポンシステムであって、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値H_1に基づいて、不可逆変換値H_i（$1 \leqq i < n$）の不可逆変換値H_{i+1}を順次計算し、上記ＵＩＤおよび不可逆変換値H_nを、１枚目のチケットとして、該消費者端末に対して送信し、

上記販売者端末のチケット発券手段は、

上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤと、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値H_1に基づいて、不可逆変換値H_i（$1 \leqq i < n$）の不可逆変換値H_{i+1}を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値H_m（$1 \leqq m \leqq n$）と、不可逆変換値H_1とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび不可逆変換値H_{m-1}を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項６】請求項１，２，３または４記載の電子クーポンシステムであって、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を計算すると共に、計算した暗号化情報H_1に基づい

て、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、上記ＵＩＤおよび暗号化情報H_nを、１枚目のチケットとして、該消費者端末に対して送信し、
上記販売者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤとを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を計算すると共に、計算した暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、受信した発券済み最新チケットのうちの暗号化情報H_m（$1 \leqq m \leqq n$）と、暗号化情報H_1とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび暗号化情報H_{m-1}を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項７】請求項１，２，３または４記載の電子クーポンシステムであって、
上記消費者端末は、
上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記販売者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記販売者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を、１枚目のチケットとして、該消費者端末に対して送信し、
上記販売者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報H_m（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、ｎ枚目のチケットである旨を示す枚数情報であるならば、ｎ枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報H_m（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるＵＩＤと、ｍ＋１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_{m+1}を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項８】請求項１，２，３，４，５，６または７記載の電子クーポンシステムであって、
上記消費者端末は、
上記販売者端末に対してパスワードを送信する際には、公開鍵暗号方式における販売者の公開鍵を用いて該パスワードを暗号化してから送信し、
上記販売者端末は、
上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における販売者の秘密鍵を用いて該パスワードを復号することを特徴とする電子クーポンシステム。
【請求項９】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末と、発券者が利用する少なくとも１つの発券者端末とが、ネットワークを介して相互に接続されてなり、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、
上記発券者端末から送信されてくるクーポンを受信するクーポン受信手段と、
上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、
上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段を備え、
上記販売者端末は、
上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段を備え、
上記発券者端末のクーポン発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を公開鍵

暗号方式における発券者の秘密鍵を用いて暗号化したデジタル署名とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、
上記販売者端末のクーポン検証手段は、
上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、
上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、
印刷されたクーポンに記載されている不可逆変換値とクーポン情報とデジタル署名とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項１０】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末と、発券者が利用する少なくとも１つの発券者端末とが、ネットワークを介して相互に接続されてなり、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、
上記発券者端末から送信されてくるクーポンを受信するクーポン受信手段と、
上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、
上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段を備え、
上記販売者端末は、
上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段を備え、
上記発券者端末のクーポン発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における発券者の秘密鍵を用いて暗号化したデジタル署名と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、
上記販売者端末のクーポン検証手段は、
上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、
該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、
上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、
印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項１１】請求項９または１０記載の電子クーポンシステムであって、
上記発券者端末のクーポン発券手段は、
作成したクーポンと共に、公開鍵暗号方式における発券者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信し、
上記消費者端末のクーポン受信手段は、
受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項１２】請求項９，１０または１１記載の電子クーポンシステムであって、
上記クーポン情報は、クーポンごとに固有のシリアル番号を含み、
上記発券者端末は、
上記販売者端末から通知されたシリアル番号を記憶するシリアル番号記憶手段と、
上記販売者端末から問い合わせがあったシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証し、検証結果を該販売者端末に対して回答するシ

リアル番号検証手段とを備え、
上記販売者端末のクーポン検証手段は、
効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を、上記発券者端末に対して通知すると共に、検証対象のクーポンに記載されているクーポン情報中のシリアル番号についての検証結果を、上記発券者端末に対して問い合わせることを特徴とする電子クーポンシステム。
【請求項１３】請求項９，１０，１１または１２記載の電子クーポンシステムであって、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記発券者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記発券者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、発券者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値H_1に基づいて、不可逆変換値H_i（$1 \leqq i < n$）の不可逆変換値H_{i+1}を順次計算し、上記ＵＩＤおよび不可逆変換値H_nを、１枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤと、発券者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値H_1に基づいて、不可逆変換値H_i（$1 \leqq i < n$）の不可逆変換値H_{i+1}を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値H_m（$1 \leqq m \leqq n$）と、不可逆変換値H_1とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび不可逆変換値H_{m-1}を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項１４】請求項９，１０，１１または１２記載の電子クーポンシステムであって、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記発券者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記発券者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）とを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を計算すると共に、計算した暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、上記ＵＩＤおよび暗号化情報H_nを、１枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤとを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を計算すると共に、計算した暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、受信した発券済み最新チケットのうちの暗号化情報H_m（$1 \leqq m \leqq n$）と、暗号化情報H_1とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび暗号化情報H_{m-1}を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項１５】請求項９，１０，１１または１２記載の電子クーポンシステムであって、

上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記発券者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、１枚目のチケットである旨を示す枚数情報とを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を、１枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報H_m（$1 \leqq m \leqq n$）を、発券者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、ｎ枚目のチケットである旨を示す枚数情報であるならば、ｎ枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報H_m（$1 \leqq m \leqq n$）を、発券者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるＵＩＤと、ｍ＋１枚目のチケットである旨を示す枚数情報とを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_{m+1}を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項１６】請求項９，１０，１１，１２，１３，１４または１５記載の電子クーポンシステムであって、
上記消費者端末は、
上記発券者端末に対してパスワードを送信する際には、公開鍵暗号方式における発券者の公開鍵を用いて該パスワードを暗号化してから送信し、また、上記販売者端末に対してパスワードを送信する際には、公開鍵暗号方式における販売者の公開鍵を用いて該パスワードを暗号化してから送信し、
上記発券者端末は、
上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における発券者の秘密鍵を用いて該パスワードを復号し、
上記販売者端末は、
上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における販売者の秘密鍵を用いて該パスワードを復号することを特徴とする電子クーポンシステム。
【請求項１７】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなるシステムにおいて、１枚で予め定めた効力を発揮するクーポンの発券および検証を行う方法であって、
クーポンの発券時に、
上記販売者端末は、
クーポンの発券を要求した消費者端末から送信されてくるパスワードを受信し、受信したパスワードと、クーポンの効力に関するクーポン情報とを、自身だけしか暗号化できない暗号化方法で暗号化し、暗号化した結果である暗号化情報と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを消費者端末に対して送信し、
クーポンの検証時に、
上記販売者端末は、
検証対象のクーポンが、上記消費者端末から送信されて使用が要求されたクーポンである場合には、
該消費者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化し、暗号化した結果と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、
検証対象のクーポンが、上記消費者端末で印刷されて使用が要求されたクーポンである場合には、
印刷されたクーポンに記載されているクーポン情報および暗号化情報を取得し、消費者から提示されたパスワードおよび取得したクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化し、暗号化した結果と、取得した暗号化情報とが一致するか否かを検証することを特徴とする電子クーポン発券・検出方法。
【請求項１８】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末と、発券者が利用する少なくとも１つの発券者端末とが、ネットワークを介して相互に接続されてなるシステムにおいて、１枚で予め定めた効力を発揮するクーポンの発券および検証を行う方法であって、
クーポンの発券時に、

上記発券者端末は、
クーポンの発券を要求した消費者端末から送信されてくるパスワードを受信し、受信したパスワードと、クーポンの効力に関するクーポン情報とを、自身だけしか暗号化できない暗号化方法で暗号化し、暗号化した結果である暗号化情報と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを消費者端末に対して送信し、
クーポンの検証時に、
上記販売者端末は、
検証対象のクーポンが、上記消費者端末から送信されて使用が要求されたクーポンである場合には、
該消費者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、上記発券者端末に対して送信して、該クーポンの検証を要求し、
検証対象のクーポンが、上記消費者端末で印刷されて使用が要求されたクーポンである場合には、
印刷されたクーポンを取得し、消費者から提示されたパスワードおよび取得したクーポンを、上記発券者端末に対して送信して、該クーポンの検証を要求し、
上記発券者端末は、
クーポンの検証を要求した販売者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化した結果と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、検証結果を該販売者端末に対して通知することを特徴とする電子クーポン発券・検出方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット等のネットワークを介して行われる電子商取引システムの利用環境において、各種商品やサービスと交換可能な電子クーポンを適正に取り扱うための電子クーポンシステムに関し、さらに詳しくは、ネットワークを介して電子クーポンを受け取った消費者が、該電子クーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようにした電子クーポンシステムに関する。

【０００２】

【従来の技術】現在、商品券や割引券等といった、各種商品やサービスと交換できる券（以下、総じて「クーポン」と称す。）が普及している。この種のクーポンには、１枚で効力を発揮するものと、複数枚だけ集めたときに効力を発揮するものとがあるが、効力が大きくなるほど、高度な印刷技術を用いることで偽造や改ざんを困難にするようにしたり、使用時に署名を確認することで第三者の不正使用を防止するようにしたりしている。

【０００３】ところで、近年の情報機器の発達と通信環境の整備により、インターネットのようなオープンなネットワークを介した電子商取引が盛んに行われるようになってきている。販売者は、ネットワーク上に仮想的な店舗を開設し、一般消費者に対して商品の販売を行う。

【０００４】このようなネットワークを介した電子商取引においても、消費者サービスの一環としてクーポン（電子クーポン）を取り扱いたいという要求が高まっている。しかし、電子クーポンを単なる画像データとした場合は、正規手順で電子クーポンを受け取った消費者が、その電子クーポンをコピーして何度も使用したり、また、他の消費者に配布したりすることが簡単にできてしまう。さらに、オープンなネットワーク経由で電子クーポンを配布することから、第三者に盗聴され不正使用されてしまうという恐れもある。

【０００５】このような不正行為を防止するための対策として、電子クーポンシステムにおいては、以下のような暗号技術が用いられている。

【０００６】第１の対策として、電子クーポンシステムにおいては、電子クーポンの偽造や改ざんを防止するために、電子クーポンに販売者（発券元）のデジタル署名を付加し、使用時にそのデジタル署名を確認するようにしている。デジタル署名技術は、例えば、「暗号理論入門：岡本栄司著，共立出版（１９９６）」の１３３頁～１３８頁に開示されている。この文献での非対称暗号（公開鍵暗号）による署名方法を簡単に説明すると、以下のようである。

【０００７】署名者は、署名したいメッセージ（または、メッセージのハッシュ値）を、署名者だけしか知らない秘密鍵を用いて暗号化することで、署名データを作成し、メッセージと署名データとをひとまとめにして検証者に渡す。検証者は、受け取った署名データを、上記秘密鍵に対応した公開鍵を用いて復号し、復号した結果と受け取ったメッセージとが一致していれば、上記署名者によって署名されたデータであると判断する。

【０００８】また、第２の対策として、電子クーポンシステムにおいては、電子クーポンの二重使用を防止するために、各電子クーポンにシリアル番号を付加し、使用時にそのシリアル番号をチェックすることで、未使用の電子クーポンであるか否かを確認するようにしている。

【０００９】さらに、第３の対策として、電子クーポンシステムにおいては、第三者による電子クーポンの不正使用を防止するために、メッセージを暗号化して送信するようにしている。メッセージを暗号化する方法としては、例えば、「ＯｐｅｎＤｅｓｉｇｎ（１９９６／６号Ｎｏ.１４）：ＣＱ出版社」の１０１頁～１１２頁に記載されているＳＳＬ（Secure Socket Layer）等が挙げられる。

【００１０】

【発明が解決しようとする課題】電子クーポンの発券から使用に至る全ての処理をネットワークを介して行うよ

うな電子クーポン専用のシステムの場合は、上述した全ての対策を講じるようにすることで、様々な不正行為を防止することができる。しかし、消費者の使い勝手を考慮すれば、消費者がネットワークを介して受け取った電子クーポンを紙に印刷し、従来の紙ベースのクーポンと同様に、販売店に持参して使用するような、紙クーポン・電子クーポン併用システムが好ましいが、そのようなシステムの場合には、電子クーポンに付加されたデジタル署名が印刷結果に反映されないことから、電子クーポンの偽造を防止することができない。

【００１１】また、使用済みシリアル番号を販売店で管理しておくことで、クーポンの二重使用を防止することはできるが、ネットワークを介して受け取った電子クーポンが消費者端末の記憶装置から盗まれた場合や、印刷されたクーポンが盗まれた場合には、そのクーポンを第三者に不正使用されてしまうと、正当な消費者がクーポンを使用することができなくなってしまう。

【００１２】さらに、複数枚だけ集めたときに効力を発揮するようなクーポン（以下、この種のクーポンを「チケット」と称す。）を取り扱う場合には、１枚で効力を発揮するクーポンに比べて発券枚数が多くなり、また、全ての消費者がチケットを集め終わるとは限らないので、消費者ごとに販売者側で管理するのは大変である。

【００１３】本発明は、上記事情に鑑みてなされたものであり、その目的は、ネットワークを介して電子クーポンを受け取った消費者が、該電子クーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようにした電子クーポンシステムを提供することにある。

【００１４】また、本発明の他の目的は、チケットを取り扱う場合に、販売者の手間を減らすことができるようにした電子クーポンシステムを提供することにある。

【００１５】

【課題を解決するための手段】上記目的を達成するために、本発明は、第１の態様として、消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなり、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、上記販売者端末は、上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、上記販売者端末のクーポン発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されている不可逆変換値とクーポン情報と暗号化情報とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、取得した暗号化情報とが一致するか否かを検証することを特徴とした電子クーポンシステムを提供している。

【００１６】第１の態様によれば、改ざんされては困るクーポン情報について、それを暗号化した暗号化情報を、目視可能なデータとして記載したクーポンを作成するようにしているので、消費者がクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されている暗号化情報を検証することで、クーポンの偽造や改ざんを防止することができるようになる。

【００１７】また、第１の態様によれば、クーポンの発券時に消費者が提示したパスワードについて、その不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしているので、クーポンの使用時に消費者が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較することで、第三者によるクーポンの不正使用を検出することができるようになる。

【００１８】なお、第１の態様において、上記販売者端末のクーポン発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における販売者の秘密鍵を用いて暗号化したデジタル署名と、上記クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポ

ンを該消費者端末に対して送信するようにしてもよく、このようにした場合は、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証するようにすることができる。

【００１９】さらに、第１の態様において、上記販売者端末のクーポン発券手段は、作成したクーポンと共に、公開鍵暗号方式における販売者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信するようにし、上記消費者端末のクーポン受信手段は、受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果とが一致するか否かを検証するようにしてもよい。

【００２０】このようにすれば、クーポンの使用時だけではなく、クーポンの発券時に、クーポンの発券を受けた消費者側で、受け取ったクーポンを検証することができるようになる。

【００２１】さらに、第１の態様において、上記クーポン情報が、クーポンごとに固有のシリアル番号を含むようにし、上記販売者端末は、効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を記憶するシリアル番号記憶手段を備えるようにし、上記販売者端末のクーポン検証手段は、検証対象のクーポンに記載されているクーポン情報中のシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証するようにしてもよい。

【００２２】このようにすれば、クーポンの偽造や改ざん、および、第三者によるクーポンの不正使用に加えて、クーポンの二重使用も防止することができるようになる。

【００２３】また、上記他の目的を達成するために、本発明は、第２の態様として、第１の態様において、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、上記販売者端末は、上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値H_1に基づいて、不可逆変換値H_i（$1 \leq i < n$）の不可逆変換値H_{i+1}を順次計算し、上記ＵＩＤおよび不可逆変換値H_nを、１枚目のチケットとして、該消費者端末に対して送信し、上記販売者端末のチケット発券手段は、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤと、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値H_1に基づいて、不可逆変換値H_i（$1 \leq i < n$）の不可逆変換値H_{i+1}を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値H_m（$1 \leq m \leq n$）と、不可逆変換値H_1とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび不可逆変換値H_{m-1}を、次のチケットとして、該消費者端末に対して送信することを特徴とした電子クーポンシステムを提供している。

【００２４】第２の態様によれば、消費者だけしか知らない情報であるパスワードと、販売者だけしか知らない秘密の情報（例えば、公開鍵暗号方式における販売者の秘密鍵）と、ｎ枚のチケットの組を識別するためのＵＩＤとを連結したものから、不可逆変換値を繰り返し計算し、ｎ番目の計算結果，ｎ－１番目の計算結果，…，２番目の計算結果，１番目の計算結果という順番で、各計算結果をチケットとして発券するようにしているので、販売店側で、消費者ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【００２５】なお、第２の態様において、上記販売者端

末の初期チケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を計算すると共に、計算した暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、上記ＵＩＤおよび暗号化情報H_nを、１枚目のチケットとして、該消費者端末に対して送信するようにし、上記販売者端末のチケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤとを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を計算すると共に、計算した暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、受信した発券済み最新チケットのうちの暗号化情報H_m（$1 \leqq m \leqq n$）と、暗号化情報H_1とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび暗号化情報H_{m-1}を、次のチケットとして、該消費者端末に対して送信するようにしてもよい。

【００２６】また、第２の態様において、上記販売者端末の初期チケット発券手段は、上述した動作ではなく、上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_1を、１枚目のチケットとして、該消費者端末に対して送信するようにし、上記販売者端末のチケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報H_m（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、ｎ枚目のチケットである旨を示す枚数情報であるならば、ｎ枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報H_m（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるＵＩＤと、ｍ＋１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報H_{m+1}を、次のチケットとして、該消費者端末に対して送信するようにしてもよい。

【００２７】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００２８】なお、以下の説明で参照する図面において、同一の符号は、同様の構成要素を表すものとする。また、これにより本発明が限定されるものではない。

【００２９】（第１の実施形態）まず、本発明の第１の実施形態について説明する。

【００３０】図１は、第１の実施形態に係る電子クーポンシステムの概略構成を示す図である。

【００３１】第１の実施形態に係る電子クーポンシステムは、消費者２００$_1$～２００$_n$（以下、単に「消費者２００」とも称す。）および販売者１００が利用するシステムであり、図１に示すように、消費者２００が利用する端末である消費者端末２０１$_1$～２０１$_n$（以下、単に「消費者端末２０１」とも称す。）と、販売者１００が利用する端末である販売者端末１０１とが、インターネット等の通信網３００を介して互いに接続されて構成されている。

【００３２】第１の実施形態に係る電子クーポンシステムにおいては、消費者２００が、消費者端末２０１を利用して、通信網３００を介して販売者端末１０１との間でデータをやり取りすることで、販売者１００に対してクーポンの発券を要求したり、販売者１００によって発券されたクーポンの使用を要求したりすることができるようにしている。このとき、販売者１００は、販売者端末１０１を利用して、消費者２００に対してクーポンを発券したり、消費者２００によって使用されるクーポンを検証したりする。

【００３３】特に、第１の実施形態に係る電子クーポンシステムにおいては、消費者２００が、消費者端末２０１を利用して、販売者１００によって発券されたクーポンを印刷し、印刷したクーポンを販売店に持参することで、直接、販売者１００に対してクーポンの使用を要求することもできるようにしている。このとき、販売者１００は、販売者端末１０１を利用して、消費者２００が持参したクーポンを検証する。

【００３４】すなわち、第１の実施形態に係る電子クーポンシステムは、通信網３００を介して行われる電子商取引環境を実現すると共に、消費者２００が、販売者１００によって発券されたクーポンを、通信網３００上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようにしたものである。

【００３５】次に、第１の実施形態に係る電子クーポンシステムを構成する販売者端末１０１および消費者端末２０１のハードウェア構成について、図２および図３を用いて説明する。

【００３６】図２は販売者端末１０１のハードウェア構成を示す図である。

【００３７】図２に示すように、販売者端末１０１は、

通信インタフェース１０２と、表示装置１０３と、入力装置１０４と、記憶装置１０５と、中央処理装置（ＣＰＵ）１０６と、一時記憶装置（メモリ）１０７とが、バス１１０によって互いに接続された構成となっている。

【００３８】通信インタフェース１０２は、通信網３００を介して、消費者端末２０１との間でデータのやり取りを行うためのインタフェースである。

【００３９】また、表示装置１０３は、販売者端末１０１を利用する販売者１００に対するメッセージ等を表示するために用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成される。

【００４０】また、入力装置１０４は、販売者端末１０１を利用する販売者１００がデータや命令等を入力するために用いられるものであり、キーボードやマウス等で構成される。

【００４１】また、記憶装置１０５は、販売者端末１０１で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【００４２】また、ＣＰＵ１０６は、販売者端末１０１の構成要素を統括的に制御したり、様々な演算処理を行ったりする。

【００４３】また、メモリ１０７には、オペレーティングシステム（以下、「ＯＳ」と称す。）１０７ａや、クーポン発券・検証処理プログラム１０７ｂといった、ＣＰＵ１０６が実行するプログラム等が一時的に格納される。

【００４４】ここで、ＯＳ１０７ａは、販売者端末１０１全体の制御を行うために、ファイル管理，プロセス管理，デバイス管理といった機能を実現するためのプログラムである。また、クーポン発券・検証処理プログラム１０７ｂは、消費者２００に対してクーポンを発券したり、消費者２００から使用が要求されたクーポンを検証したりするためのプログラムである。

【００４５】図３は消費者端末２０１のハードウェア構成を示す図である。

【００４６】図３に示すように、消費者端末２０１は、通信インタフェース２０２と、表示装置２０３と、入力装置２０４と、記憶装置２０５と、中央処理装置（ＣＰＵ）２０６と、一時記憶装置（メモリ）２０７と、印刷装置２０８とが、バス２１０によって互いに接続された構成となっている。

【００４７】通信インタフェース２０２は、通信網３００を介して、販売者端末１０１との間でデータのやり取りを行うためのインタフェースである。

【００４８】また、表示装置２０３は、消費者端末２０１を利用する消費者２００に対するメッセージ等を表示するために用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成される。

【００４９】また、入力装置２０４は、消費者端末２０１を利用する消費者２００がデータや命令等を入力するために用いられるものであり、キーボードやマウス等で構成される。

【００５０】また、記憶装置２０５は、消費者端末２０１で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【００５１】また、ＣＰＵ２０６は、消費者端末２０１の構成要素を統括的に制御したり、様々な演算処理を行ったりする。

【００５２】また、メモリ２０７には、ＯＳ２０７ａや、クーポン要求・受信・発信処理プログラム２０７ｂといった、ＣＰＵ２０６が実行するプログラム等が一時的に格納される。

【００５３】ここで、ＯＳ２０７ａは、消費者端末２０１全体の制御を行うために、ファイル管理，プロセス管理，デバイス管理といった機能を実現するためのプログラムである。また、クーポン要求・受信・発信処理プログラム２０７ｂは、販売者１００に対してクーポンの発券を要求したり、販売者１００によって発券されたクーポンを受信したり、販売者１００に対してクーポンの使用を要求したりするためのプログラムである。

【００５４】また、印刷装置２０８は、電子的なデータを印刷するために用いられるものであり、プリンタ等で構成される。

【００５５】次に、第１の実施形態に係る電子クーポンシステムの動作について説明する。

【００５６】なお、以下の説明おいて、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、販売者１００が行う処理は、実際には、販売者１００の指示によって販売者端末１０１が実行するものである。

【００５７】図４は、消費者２００が、販売者１００に対してクーポンの発券を要求し、販売者１００によって発券されたクーポンを受信するまでの動作を説明するための図である。

【００５８】図４において、まず、消費者２００は、販売者１００からクーポンの発券を受ける条件を満たしているものとする（Ｓ２０００）。

【００５９】消費者２００は、後述するクーポン要求処理（Ｓ２４００）を行い、暗号化した自身のパスワード５０１を、販売者１００に対して送信する。

【００６０】販売者１００は、パスワード５０１を受信すると、後述するクーポン発券処理（Ｓ１３００）を行い、クーポン５０２と、クーポン５０２のデジタル署名５０３とを、消費者２００に対して送信する。

【００６１】消費者２００は、クーポン５０２およびデジタル署名５０３を受信すると、後述するクーポン受信処理（Ｓ２５００）を行い、受信したクーポン５０２を保管する。

【００６２】図５は、既にクーポンの発券を受けている消費者２００が、通信網３００を介してクーポンを使用し、販売者１００が、クーポンを検証するまでの動作を説明するための図である。

【００６３】図５において、既にクーポンの発券を受けている消費者２００は、後述するクーポン使用オンライン処理（Ｓ２６００）を行い、クーポン受信処理（Ｓ２５００）で入手したクーポン５０２と、暗号化した自身のパスワード５０１とを、販売者１００に対して送信する。

【００６４】販売者１００は、クーポン５０２およびパスワード５０１を受信すると、後述するクーポン検証処理（Ｓ１４００）を行い、受信したクーポン５０２を検証する。

【００６５】図６は、既にクーポンの発券を受けている消費者２００が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者１００が、クーポンを検証するまでの動作を説明するための図である。

【００６６】図６において、既にクーポンの発券を受けている消費者２００は、後述するクーポン使用オフライン処理（Ｓ２７００）を行い、印刷されたクーポン５０４を販売店に持参する。

【００６７】販売者１００は、消費者２００が持参したクーポン５０４を受け取ると、クーポン検証処理（Ｓ１４００）を行い、受け取ったクーポン５０４を検証する。

【００６８】図７は、図４のクーポン要求処理（Ｓ２４００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００６９】図７に示すように、クーポン要求処理（Ｓ２４００）において、消費者２００は、まず、販売者１００に対して、公開鍵暗号方式における販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２４０１）。

【００７０】続いて、消費者２００は、自身だけしか知らないパスワードを入力する（ステップ２４０２）。

【００７１】続いて、消費者２００は、ステップ２４０２で入力したパスワードを、ステップ２４０１で入手した公開鍵を用いて暗号化し（ステップ２４０３）、暗号化したパスワード５０１を、販売者１００に対して送信する（ステップ２４０４）。

【００７２】図８は、図４のクーポン発券処理（Ｓ１３００）の処理フローチャートであり、本処理は、クーポン発券・検証処理プログラム１０７ｂによって実現される。

【００７３】図８に示すように、クーポン発券処理（Ｓ１３００）において、販売者１００は、まず、暗号化されたパスワード５０１を受信すると（ステップ１３０１）、受信したパスワード５０１を、公開鍵暗号方式における販売者１００の秘密鍵を用いて復号する（ステップ１３０２）。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網３００を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【００７４】続いて、販売者１００は、ステップ１３０２で復号したパスワード５０１に不可逆変換を施す（ステップ１３０３）。以下、パスワードに不可逆変換を施した結果を、パスワードの不可逆変換値またはＰＨと称す。

【００７５】続いて、販売者１００は、シリアル番号，有効期限，クーポンの価値（例えば、金額）等の、クーポンの効力に関するクーポン情報を設定し（ステップ１３０４）、設定したクーポン情報のデジタル署名を、販売者１００の秘密鍵を用いて計算する（ステップ１３０５）。そして、ステップ１３０３で計算した不可逆変換値，ステップ１３０４で設定したクーポン情報，ステップ１３０５で計算したデジタル署名を、目視可能なデータ（例えば、数字や文字等）として記載したクーポンを作成することで、書面としてのクーポン５０２を作成する（ステップ１３０６）。

【００７６】続いて、販売者１００は、書面としてのクーポン５０２全体のデジタル署名５０３を、販売者１００の秘密鍵を用いて計算し（ステップ１３０７）、ステップ１３０６で作成したクーポン５０２と、ステップ１３０７で計算したデジタル署名５０３とを、消費者２００に対して送信する（ステップ１３０８）。

【００７７】図９は、図４のクーポン受信処理（Ｓ２５００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００７８】図９に示すように、クーポン受信処理（Ｓ２５００）において、消費者２００は、販売者１００が送信したクーポン５０２およびデジタル署名５０３を受信すると（ステップ２５０１）、受信したデジタル署名５０３を検証することで、受信したクーポン５０２が、通信網３００を介して送信されてくる間に改ざんされていないか否かを検証する（ステップ２５０２）。ステップ２５０２では、詳しくは、消費者２００は、受信したクーポン５０２と、受信したデジタル署名５０３を販売者１００の公開鍵を用いて復号した結果とを比較し、両者が一致すれば、受信したクーポン５０２が改ざんされていないと判断する。

【００７９】そして、改ざんされていないならば、受信したクーポン５０２を記憶装置２０５に保存する（ステップ２５０３）。

【００８０】ここで、クーポン５０２は、例えば、図１４に示すような形式とすることができ、受信時に表示装置２０３に表示されるようにすることが好ましい。

【００８１】図１０は、図５のクーポン使用オンライン

処理（Ｓ２６００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００８２】図１０に示すように、クーポン使用オンライン処理（Ｓ２６００）において、消費者２００は、まず、販売者１００に対して、販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２６０１）。

【００８３】続いて、消費者２００は、自身だけしか知らないパスワード（クーポン要求処理（Ｓ２４００）で入力したパスワードと同一のパスワード）を入力する（ステップ２６０２）。

【００８４】続いて、消費者２００は、ステップ２６０２で入力したパスワードを、ステップ２６０１で入手した公開鍵を用いて暗号化し（ステップ２６０３）、暗号化したパスワード５０１と、図９に示したクーポン受信処理（Ｓ２５００）で入手したクーポン５０２とを、販売者１００に対して送信する（ステップ２６０４）。

【００８５】図１１は、図６のクーポン使用オフライン処理（Ｓ２７００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００８６】図１１に示すように、クーポン使用オフライン処理（Ｓ２７００）において、消費者２００は、図９に示したクーポン受信処理（Ｓ２５００）で入手したクーポン５０２を、印刷装置２０８で印刷する（ステップ２７０１）。

【００８７】ここで、印刷されたクーポン５０４の形式は、図１４に示したクーポン５０２の形式と同様の形式である。

【００８８】続いて、消費者２００は、印刷されたクーポン５０４を販売店に持参し、自身だけしか知らないパスワード（クーポン要求処理（Ｓ２４００）で入力したパスワードと同一のパスワード）を、販売者１００に告げる（ステップ２７０２）。なお、ステップ２７０２は、消費者２００自身が行う行動であり、消費者端末２０１では実行されない。

【００８９】図１２は、図５および図６のクーポン検証処理（Ｓ１４００）の処理フローチャートであり、本処理は、クーポン発券・検証処理プログラム１０７ｂによって実現される。

【００９０】図１２に示すように、クーポン検証処理（Ｓ１４００）は、使用されるクーポンが、通信網３００を介してオンラインで届いたクーポン５０２であるか、または、直接持参されたクーポン（印刷されたクーポン）５０４であるかによって、処理が分かれる（ステップ１４０１）。

【００９１】直接持参されたクーポン５０４である場合には、販売者１００は、ステップ１４０４の書面検証処理から処理を開始する。ただし、このとき、販売者１００は、クーポン５０４に記載されている各種情報を取得する必要があるが、取得方法については任意である。

【００９２】また、通信網３００を介してオンラインで届いたクーポン５０２である場合には、販売者１００は、このクーポン５０２と共に、暗号化されたパスワード５０１を受信し（ステップ１４０２）、受信したパスワード５０１を、販売者１００の秘密鍵を用いて復号する（ステップ１４０３）。

【００９３】ステップ１４０４では、販売者１００は、クーポンに記載されている各種情報を検証する書面検証処理を行う。なお、書面検証処理の詳細については後述する。

【００９４】ステップ１４０４の書面検証処理の結果、全ての情報についての検証に合格した場合には（ステップ１４０５）、クーポンの二重使用を防止するために、クーポンに記載されているクーポン情報中のシリアル番号を、使用済みシリアル番号リストに登録し（ステップ１４０６）、クーポンの定められた効力を発揮させる（ステップ１４０７）。また、１つでも不合格であった場合には（ステップ１４０５）、エラー処理を実行する（ステップ１４０８）。

【００９５】図１３は、図１２の書面検証処理（ステップ１４０４）の処理フローチャートである。

【００９６】図１３に示すように、書面検証処理（ステップ１４０４）において、販売者１００は、まず、書面としてのクーポンに記載されているクーポン情報のデジタル署名を、販売者１００の秘密鍵を用いて計算する（ステップ１４１０）。

【００９７】そして、検証に合格しなければ（ステップ１４１１）、すなわち、計算したデジタル署名と、クーポンに記載されているデジタル署名とが一致しなければ、クーポンが改ざんされているので、エラー処理を実行する（ステップ１４１７）。

【００９８】また、検証に合格すれば（ステップ１４１１）、すなわち、計算したデジタル署名と、クーポンに記載されているデジタル署名とが一致すれば、ステップ１４０３で得たパスワード（または、消費者２００から告げられたパスワード）の不可逆変換値を計算し、計算した不可逆変換値と、書面としてのクーポンに記載されている不可逆変換値と比較する（ステップ１４１２）。

【００９９】ステップ１４１２の比較の結果、両者が一致しなければ（ステップ１４１３）、クーポン発券時のパスワードを知らない第三者によるクーポンの不正使用であると考えられるので、エラー処理を実行する（ステップ１４１８）。

【０１００】また、販売者１００は、書面としてのクーポンに記載されているクーポン情報中のシリアル番号が、使用済みシリアル番号リストに登録されているか否かを検証する（ステップ１４１４）。既に登録されているならば（ステップ１４１５）、クーポンの二重使用という理由で、エラー処理を実行する（ステップ１４１

9）。

【０１０１】最後に、販売者１００は、書面としてのクーポンに記載されているクーポン情報中の有効期限を参照し、有効期限内のクーポンであるか否かを検証し（ステップ１４１６）、有効期限外であれば、有効期限切れのエラー処理を実行する（ステップ１４２０）。

【０１０２】これら全ての検証に合格すれば、クーポンは有効となり、効力が発揮されることとなる。

【０１０３】以上説明したように、第１の実施形態に係る電子クーポンシステムにおいては、シリアル番号，有効期限，金額等の改ざんされては困るクーポン情報のデジタル署名を、販売者１００だけしか知らない情報である秘密鍵を用いて計算し、計算したデジタル署名を、目視可能なデータとして記載したクーポンを作成するようにしている。

【０１０４】従って、第１の実施形態に係る電子クーポンシステムによれば、消費者２００が電子的なクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されているデジタル署名を検証することで、クーポンの偽造や改ざんを検出することができる。

【０１０５】また、第１の実施形態に係る電子クーポンシステムにおいては、クーポンの発券時に、消費者２００が提示したパスワードの不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしている。さらに、クーポンの使用時には、発券を要求した消費者２００だけしか知らないパスワードを販売者１００に提示し、消費者２００が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較するようにしている。

【０１０６】従って、第１の実施形態に係る電子クーポンシステムによれば、たとえクーポンが盗まれたとしても、クーポンの発券要求時に提示されたパスワードを知らない第三者がクーポンを不正使用するのを防止することができる。

【０１０７】なお、第１の実施形態に係る電子クーポンシステムにおいては、クーポン情報について、公開鍵暗号方式における販売者１００の秘密鍵を用いて計算したデジタル署名を、目視可能なデータとしてクーポンに記載するようにした例を示しているが、販売者１００だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにしてもよい。

【０１０８】また、第１の実施形態に係る電子クーポンシステムにおいては、パスワードについて、不可逆変換を施した不可逆変換値を、目視可能なデータとしてクーポンに記載するようにした例を示しており、本例によれば、不可逆変換方法を公開しても支障がないので、パスワードの不可逆変換値が不一致である場合に、消費者２００が、自身が提示したパスワードの不可逆変換値を計算して確認することが可能である。しかしながら、パスワードについて、販売者１００だけしか暗号化できない暗号化方法で暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにしてもよい。

【０１０９】なお、本発明は、上述した第１の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【０１１０】例えば、第１の実施形態に係る電子クーポンシステムにおいては、消費者２００は、販売者１００に対してパスワードを送信するときに、販売者１００の公開鍵を取得し、暗号通信を行うようにしているが、本発明はこれに限定しない。消費者２００は、１度、販売者１００の公開鍵を入手すれば、２回以降は、その公開鍵を使うことができる。また、販売者１００と消費者２００との間で共通の鍵を持つことができれば、秘密鍵暗号技術を使って暗号化するようにしてもよい。

【０１１１】また、第１の実施形態に係る電子クーポンシステムにおいて、消費者２００から販売者１００に対してパスワードを送信するときに、暗号化されたパスワードがそのまま盗まれて不正使用されるのを防止するために、パスワードを、その他の情報（乱数や適当な数字でよい。）と共に暗号化して送信するようにしてもよい。

【０１１２】また、第１の実施形態に係る電子クーポンシステムにおいては、販売者１００は、デジタル署名を、数値や文字等の目視可能なデータとしてクーポンに記載するようにしているが、印刷後に目視可能であれば、例えば、バーコード等のようなものであってもよい。バーコードとして記載すれば、販売者１００は、印刷されたクーポンから各種情報を取得する際に、バーコードリーダを用いることができるようになる。

【０１１３】また、第１の実施形態に係る電子クーポンシステムにおいては、販売者１００は、消費者２００のパスワードの不可逆変換値と、シリアル番号，有効期限，金額等のクーポン情報のデジタル署名とを、別々にクーポンに記載するようにしているが、クーポン情報と共に、パスワードも一緒にデジタル署名を計算するようにしてもよい。また、このとき、クーポン情報やパスワード等の、デジタル署名を計算する元の情報は、不可逆変換を施した後に、デジタル署名を計算するようにしてもよい。

【０１１４】（第２の実施形態）ところで、クーポンは、販売者１００の販売方針により、１枚で効力を発揮するものと、ある種の条件を満たしたときのみ、効力を発揮するものとがある。例えば、予め定めた枚数だけ集めたときに効力を発揮するようなクーポン（以下、この種のクーポンを、特に「チケット」と称す。）を取り扱うようにした場合を、第２の実施形態として、上述した第１の実施形態と異なる点についてのみ説明する。

【０１１５】第２の実施形態に係る電子クーポンシステ

ムの概略構成は、図１に示した概略構成と同様である。

【０１１６】図１５は販売者端末１０１のハードウェア構成を示す図である。

【０１１７】図２に示したハードウェア構成と異なる点は、メモリ１０７に、チケット発券・検証処理プログラム１０７ｃが一時的に格納される点である。

【０１１８】チケット発券・検証処理プログラム１０７ｃは、消費者２００に対してチケットを発券したり、消費者２００から使用が要求されたチケットを検証したりするためのプログラムである。

【０１１９】図１６は消費者端末２０１のハードウェア構成を示す図である。

【０１２０】図３に示したハードウェア構成と異なる点は、メモリ２０７に、チケット要求・受信・発信処理プログラム２０７ｃが一時的に格納される点である。

【０１２１】チケット要求・受信・発信処理プログラム２０７ｃは、販売者１００に対してチケットの発券を要求したり、販売者１００によって発券されたチケットを受信したり、販売者１００に対してチケットの使用を要求したりするためのプログラムである。

【０１２２】次に、第２の実施形態に係る電子クーポンシステムの動作について説明する。

【０１２３】なお、以下の説明おいても、上述した第１の実施形態と同様に、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、販売者１００が行う処理は、実際には、販売者１００の指示によって販売者端末１０１が実行するものである。

【０１２４】図１７は、消費者２００が、販売者１００に対して１枚目のチケットの発券を要求し、販売者１００によって発券された１枚目のチケットを受信するまでの動作を説明するための図である。なお、チケットは、ｎ枚だけ集めたときに効力を発揮するものとする。

【０１２５】図１７において、まず、消費者２００は、後述する初期チケット発券要求処理（Ｓ２１００）を行い、暗号化した自身のパスワード５０１を、販売者１００に対して送信する。

【０１２６】販売者１００は、パスワード５０１を受信すると、後述する初期チケット発券処理（Ｓ１１００）を行い、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）５０５と、受信したパスワード５０１，ＵＩＤ５０５，販売者１００だけしか知らない秘密の情報（例えば、販売者１００の秘密鍵）を連結したものの、ｎ番目の不可逆変換値H_n(506_n)とを、１枚目のチケットとして、消費者２００に対して送信する。

【０１２７】消費者２００は、ＵＩＤ５０５およびH_n(506_n)を受信すると、後述するチケット受信処理（Ｓ２２００）を行い、受信したＵＩＤ５０５およびH_n(506_n)を保管する。

【０１２８】図１８は、消費者２００が、販売者１００に対して２枚目以降のチケットの発券を要求し、販売者１００によって発券された２枚目以降のチケットを受信するまでの動作を説明するための図である。

【０１２９】図１８において、まず、消費者２００は、２枚目のチケットの発券を受ける場合は、後述するチケット発券要求処理（Ｓ２３００）を行い、暗号化した自身のパスワード５０１と、１枚目のチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５およびH_n(506_n)とを、販売者１００に対して送信する。

【０１３０】販売者１００は、パスワード５０１，ＵＩＤ５０５，H_n(506_n)を受信すると、後述するチケット発券処理（Ｓ１２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，H_n(506_n)と、販売者１００の秘密鍵とから、H_{n-1}(506_{n-1})を求めて、求めたH_{n-1}(506_{n-1})を、２枚目のチケットとして、消費者２００に対して送信する。

【０１３１】消費者２００は、H_{n-1}(506_{n-1})を受信すると、チケット受信処理（Ｓ２２００）を行い、受信したH_{n-1}(506_{n-1})を保管する。

【０１３２】同様に、消費者２００は、ｍ＋１枚目（$1 \leqq m < n$）のチケットの発券を受ける場合は、チケット発券要求処理（Ｓ２３００）を行い、暗号化した自身のパスワード５０１と、ｍ枚目のチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５および$H_{n-(m-1)}$($506_{n-(m-1)}$)とを、販売者１００に対して送信する。

【０１３３】販売者１００は、パスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}$($506_{n-(m-1)}$)を受信すると、チケット発券処理（Ｓ１２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}$($506_{n-(m-1)}$)と、販売者１００の秘密鍵とから、H_{n-m}(506_{n-m})を求めて、求めたH_{n-m}(506_{n-m})を、ｍ＋１枚目のチケットとして、消費者２００に対して送信する。

【０１３４】消費者２００は、H_{n-m}(506_{n-m})を受信すると、チケット受信処理（Ｓ２２００）を行い、受信したH_{n-m}(506_{n-m})を保管する。

【０１３５】このようにして、消費者２００は、ｎ枚のチケットを集めることができ、これらｎ枚のチケットの効力を発揮させたい場合には、チケット発券要求処理（Ｓ２３００）を行い、暗号化された自身のパスワード５０１と、ｎ枚目のチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５およびH_1(506_1)とを、販売者１００に対して送信する。

【０１３６】販売者１００は、パスワード５０１，ＵＩＤ５０５，H_1(506_1)を受信すると、チケット発券処理（Ｓ１２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，H_1(506_1)と、販売者１００の秘密鍵とから、消費者２００がｎ枚だけチケットを集めたことを確認し、ｎ枚のチケット収集終了処理（Ｓ１２５０）を行う。

【０１３７】図１９は、図１７の初期チケット発券要求処理（Ｓ２１００）の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム２０７ｃによって実現される。

【０１３８】図１９に示すように、初期チケット発券要求処理（Ｓ２１００）において、消費者２００は、まず、販売者１００に対して、販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２１０１）。

【０１３９】続いて、消費者２００は、自身だけしか知らないパスワードを入力する（ステップ２１０２）。

【０１４０】続いて、消費者２００は、ステップ２１０２で入力したパスワードを、ステップ２１０１で入手した公開鍵を用いて暗号化し（ステップ２１０３）、暗号化したパスワード５０１を、販売者１００に対して送信する（ステップ２１０４）。

【０１４１】図２０は、図１７の初期チケット発券処理（Ｓ１１００）の処理フローチャートであり、本処理は、チケット発券・検証処理プログラム１０７ｃによって実現される。

【０１４２】図２０に示すように、初期チケット発券処理（Ｓ１１００）において、販売者１００は、まず、暗号化されたパスワード５０１を受信すると（ステップ１１０１）、受信したパスワード５０１を、販売者１００の秘密鍵を用いて復号する（ステップ１１０２）。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網３００を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【０１４３】続いて、販売者１００は、ｎ枚のチケットの組を識別するための固有の値であるＵＩＤ５０５を作成し（ステップ１１０３）、ステップ１１０２で復号したパスワード，ステップ１１０３で作成したＵＩＤ５０５，販売者１００の秘密鍵を結合したものに、不可逆変換を施す（ステップ１１０４）。以下、パスワード，ＵＩＤ，秘密鍵を結合したものに不可逆変換を施した結果を、不可逆変換値H_m（$1 \leqq m \leqq n$）と称すが、ステップ１１０４で計算される不可逆変換値H_mはH_1（506_1）である。

【０１４４】続いて、販売者１００は、H_iの不可逆変換値H_{i+1}（$1 \leqq i < n$）を計算する（ステップ１１０５）。ステップ１１０５では、詳しくは、販売者１００は、図２４に示すように、まず、H_1（506_1）の不可逆変換値H_2（506_2）を計算し、H_{n-1}（506_{n-1}）の不可逆変換値H_n（506_n）を計算するまで、H_iの不可逆変換値H_{i+1}（$1 \leqq i < n$）を繰り返し計算する。

【０１４５】最後に、販売者１００は、ステップ１１０３で作成したＵＩＤ５０５と、ｎ番目の不可逆変換値H_n（506_n）とを、１枚目のチケットとして、消費者２００に対して送信する（ステップ１１０６）。

【０１４６】図２１は、図１７および図１８のチケット受信処理（Ｓ２２００）の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム２０７ｃによって実現される。

【０１４７】図２１に示すように、チケット受信処理（Ｓ２２００）において、消費者２００は、販売者１００から送信されてきたデータを受信すると（ステップ２２０１）、受信したデータにＵＩＤ５０５が含まれているか否かを判定し（ステップ２２０２）、含まれている場合には、ＵＩＤ５０５を記憶装置２０５に保存する（ステップ２２０３）。

【０１４８】最後に、消費者２００は、受信した不可逆変換値H_mを記憶装置２０５に保存する（ステップ２２０４）。

【０１４９】なお、消費者２００は、受信した不可逆変換値H_mを記憶装置２０５に保存した回数をカウントすることで、何枚目のチケットが発券されたかを認識することができる。そこで、消費者端末２０１において、何枚目のチケットが発券されたかを示す表示が表示装置２０３になされるようにすることが好ましい。

【０１５０】図２２は、図１８のチケット発券要求処理（Ｓ２３００）の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム２０７ｃによって実現される。

【０１５１】図２２に示すように、チケット発券要求処理（Ｓ２３００）において、消費者２００は、まず、販売者１００に対して、販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２３０１）。

【０１５２】続いて、消費者２００は、自身だけしか知らないパスワード（初期チケット発券要求処理（Ｓ２１００）で入力したパスワードと同一のパスワード）を入力する（ステップ２３０２）。

【０１５３】続いて、消費者２００は、ステップ２３０２で入力したパスワードを、ステップ２３０１で入手した公開鍵を用いて暗号化し（ステップ２３０３）、暗号化したパスワード５０１と、図２１に示したチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５と、１回前のチケット受信処理（Ｓ２２００）で入手した不可逆変換値H_mとを、販売者１００に対して送信する（ステップ２３０４）。

【０１５４】このように、１回前のチケット受信処理（Ｓ２２００）で入手した不可逆変換値H_mを送信することによって、販売者１００は、消費者２００に発券した最新のチケットが何枚目であるか、すなわち、消費者２００が何枚目までのチケットを集めているかを知ることができるようになる。

【０１５５】なお、消費者２００は、１枚目のチケットの発券を要求すべきであるか（図１９に示した初期チケット発券要求処理（Ｓ２１００）を行うべきであるか）、または、２枚目以降のチケットの発券を要求すべきであるか（図２２に示したチケット発券要求処理（Ｓ

２３００）を行うべきであるか）については、記憶装置２０５にＵＩＤ５０５が記憶されているか否かで判断することができる。

【０１５６】図２３は、図１８のチケット発券処理（Ｓ１２００）の処理フローチャートであり、本処理は、チケット発券・検証処理プログラム１０７ｃによって実現される。

【０１５７】図２３に示すように、チケット発券処理（Ｓ１２００）において、販売者１００は、まず、暗号化されたパスワード５０１，ＵＩＤ５０５，不可逆変換値H_mを受信すると（ステップ１２０１）、受信したパスワード５０１を、販売者１００の秘密鍵を用いて復号する（ステップ１２０２）。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網３００を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【０１５８】続いて、販売者１００は、ステップ１２０２で復号したパスワード，ステップ１２０１で受信したＵＩＤ５０５，販売者１００の秘密鍵を結合したもの、不可逆変換値H_1を計算する（ステップ１２０３）。

【０１５９】続いて、販売者１００は、ステップ１２０１で受信したH_mとステップ１２０３で計算したH_1とが一致するか否かを検証し（ステップ１２０４）、一致した場合は、消費者２００がｎ枚のチケットを集め終えたことを意味しているので、ステップ１２０８に進んで、チケット収集完了処理を行う。なお、ステップ１２０８のチケット収集完了処理は、図１８のチケット収集終了処理（Ｓ１２５０）に相当しており、その処理内容は、販売者１００の販売方針に応じた様々な処理内容が考えられ、特に定めるものではない。

【０１６０】また、販売者１００は、ステップ１２０１で受信したH_mとステップ１２０３で計算したH_1とが一致しない場合は（ステップ１２０４）、消費者２００がｎ枚のチケットを集め終えていないことを意味しているので、H_iの不可逆変換値H_{i+1}（$1 \leqq i < n$）を計算し（ステップ１２０５）、$H_m = H_i$となるｉ（$1 < i \leqq n$）を求める（ステップ１２０６）。なお、ステップ１２０６では、販売者１００は、図２０に示した初期チケット発券処理（Ｓ１１００）のステップ１１０５と同様にして、H_iの不可逆変換値H_{i+1}（$1 \leqq i < n$）を繰り返し計算するが、$H_m = H_i$となるｉ（$1 < i \leqq n$）が求まった時点で、計算を中止することができる。

【０１６１】ここで、$H_m = H_i$となるｉが存在しない場合は、ステップ１２０１で受信したパスワード５０１，ＵＩＤ５０５，Ｈｍの少なくともいずれかが不正であることを意味しているので、エラー処理を実行する（ステップ１２０９）。

【０１６２】また、販売者１００は、$H_m = H_i$となるｉが存在する場合は、ＵＩＤ５０５と共に、H_{i-1}を、消費者２００に対して送信する（ステップ１２０７）。

【０１６３】以上説明したように、第２の実施形態に係る電子クーポンシステムにおいては、チケットの発券時に、販売者１００だけしか知らない秘密の情報である販売者１００の秘密鍵，消費者２００だけしか知らない情報であるパスワード，ｎ枚のチケットの組を識別するためのＵＩＤを連結したものから、不可逆変換値を繰り返し計算し、ｎ番目の不可逆変換値H_n，ｎ－１番目の不可逆変換値H_{n-1}，…，２番目の不可逆変換値H_2，１番目の不可逆変換値H_1という順番で、各不可逆変換値を消費者２００に対して返信するようにしている。また、消費者２００から販売者１００に対して、１回前に送信されたH_m，ＵＩＤ，パスワードを送信するようにしている。また、不可逆変換値を計算するのに必要な消費者２００ごとのデータは、消費者２００から販売者１００に対して送信されるようにしている。

【０１６４】従って、第２の実施形態に係る電子クーポンシステムによれば、上述した第１の実施形態による効果に加えて、たとえチケットが通信路上で盗まれたとしても、パスワードを知らない第三者がチケットを不正使用するのを防止することができると共に、販売者１００側で、消費者２００ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【０１６５】なお、第２の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【０１６６】例えば、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、販売者１００の秘密鍵を用いて不可逆変換値を計算するようにしているが、この計算は、販売者１００以外が計算不可能であればよいので、不可逆変換のアルゴリズムが非公開であれば、販売者１００の秘密鍵を用いなくてもよい。

【０１６７】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００が、初期チケット発券時に、消費者２００に対してＵＩＤを送信し、消費者２００が、そのＵＩＤを保管しておき、その後は、保管しておいたＵＩＤを消費者２００から販売者１００に対して送信するようにしているが、チケット発券時に、その都度、販売者１００から消費者２００に対してＵＩＤを送信するようにしてもよい。

【０１６８】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、販売者１００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワードおよびＵＩＤを連結したものを、販売者１００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における販売者１００の秘密鍵）を用いて暗号化し、暗号化した暗号化

情報を、消費者２００に対して返信するようにしてもよい。詳しくは、販売者１００は、パスワードおよびＵＩＤを連結したものの暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、ｎ番目の暗号化情報H_n，ｎ－１番目の暗号化情報H_{n-1}，…，２番目の暗号化情報H_2，１番目の暗号化情報H_1という順番で、各暗号化情報を消費者２００に対して返信するようにしてもよい。

【０１６９】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、販売者１００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワード，ＵＩＤ，何枚目のチケットであるかを示す枚数情報を連結したものを、販売者１００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における販売者１００の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者２００に対して返信するようにしてもよい。このようにすれば、販売者１００は、消費者２００からチケットの発券要求時に送信されてくる暗号化情報を、販売者１００だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報によって、消費者２００が何枚のチケットを集めたかを知ることができる。

【０１７０】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、不可逆変換値を消費者２００に対して送信するようにしているが、上述した第１の実施形態で説明したクーポンと同様に、不可逆変換値を目視可能なデータとして記載したチケットを作成し、書面としてのチケットを消費者２００に対して送信するようにしてもよい。このようにすれば、消費者端末２０１においては、例えば、図２５に示すような表示が表示装置２０３になされて、何枚目のチケットが発券されたかを示すようにすることができる。

【０１７１】さらに、第２の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したクーポンと同様に、販売者１００から消費者２００に対して、チケットと共に、チケット全体のデジタル署名が送信されるようにしてもよく、このようにすれば、チケットの発券を受けた消費者２００側で、受け取ったチケットが改ざんされていないか否かを検証することができる。

【０１７２】（第３の実施形態）ところで、クーポンの発券を、販売者１００とは別に設けた専用の発券者が行うようにしてもよく、以下、クーポンの発券者を設けるようにした場合を、第３の実施形態として、上述した第１の実施形態と異なる点についてのみ説明する。

【０１７３】図２６は、第３の実施形態に係る電子クーポンシステムの概略構成を示す図である。

【０１７４】第３の実施形態に係る電子クーポンシステムは、消費者200_1～200_n（以下、単に「消費者２００」とも称す。），販売者端末600_1～600_n（以下、単に「販売者６００」とも称す。），発券者７００が利用するシステムであり、図２６に示すように、消費者２００が利用する端末である消費者端末201_1～201_n（以下、単に「消費者端末２０１」とも称す。）と、販売者６００が利用する端末である販売者端末601_1～601_n（以下、単に「販売者端末６０１」とも称す。）と、発券者７００が利用する端末である発券者端末７０１とが、インターネット等の通信網３００を介して互いに接続されて構成されている。

【０１７５】次に、第３の実施形態に係る電子クーポンシステムを構成する発券者端末７０１および販売店端末６０１のハードウェア構成について、図２７および図２８を用いて説明する。なお、消費者端末２０１のハードウェア構成は、図３に示したハードウェア構成と同様である。

【０１７６】図２７は発券者端末７０１のハードウェア構成を示す図である。

【０１７７】図２７に示すように、発券者端末７０１は、通信インタフェース７０２と、表示装置７０３と、入力装置７０４と、記憶装置７０５と、中央処理装置（ＣＰＵ）７０６と、一時記憶装置（メモリ）７０７とが、バス７１０によって互いに接続された構成となっており、基本的には、図２に示した販売者端末１０１のハードウェア構成と同様である。

【０１７８】メモリ７０７には、ＯＳ７０７ａや、クーポン発券・検証処理プログラム７０７ｂといった、ＣＰＵ７０６が実行するプログラム等が一時的に格納される。

【０１７９】ここで、ＯＳ７０７ａは、発券者端末７０１全体の制御を行うために、ファイル管理，プロセス管理，デバイス管理といった機能を実現するためのプログラムである。また、クーポン発券・検証処理プログラム７０７ｂは、消費者２００に対してクーポンを発券したり、販売者６００から検証（後述するように、クーポンの二重使用についての検証である。）が要求されたクーポンを検証したりするためのプログラムである。

【０１８０】図２８は販売者端末６０１のハードウェア構成を示す図である。

【０１８１】図２に示したハードウェア構成と異なる点は、メモリ１０７に、クーポン発券・検証処理プログラム１０７ｂの代わりに、クーポン検証処理プログラム６０７ｂが一時的に格納される点である。

【０１８２】クーポン検証処理プログラム６０７ｂは、消費者２００から使用が要求されたクーポンを検証するためのプログラムである。

【０１８３】次に、第３の実施形態に係る電子クーポンシステムの動作について説明する。

【０１８４】なお、以下の説明おいても、上述した第１

の実施形態と同様に、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、販売者６００が行う処理は、実際には、販売者６００の指示によって販売者端末６０１が実行するものであり、さらに、発券者７００が行う処理は、実際には、発券者７００の指示によって発券者端末７０１が実行するものである。

【０１８５】図２９は、消費者２００が、発券者７００に対してクーポンの発券を要求し、発券者７００によって発券されたクーポンを受信するまでの動作を説明するための図である。

【０１８６】図２９において、まず、消費者２００は、発券者７００からクーポンの発券を受ける条件を満たしているものとする（Ｓ２０００）。

【０１８７】消費者２００は、後述するクーポン要求処理（Ｓ１２４００）を行い、暗号化した自身のパスワード５０１を、発券者７００に対して送信する。

【０１８８】発券者７００は、パスワード５０１を受信すると、後述するクーポン発券処理（Ｓ７３００）を行い、クーポン５０２と、クーポン５０２のデジタル署名５０３とを、消費者２００に対して送信する。

【０１８９】消費者２００は、クーポン５０２およびデジタル署名５０３を受信すると、後述するクーポン受信処理（Ｓ１２５００）を行い、受信したクーポン５０２を保管する。

【０１９０】図２９に示した動作は、図４に示した動作において、販売者１００が発券者７００に代わっている点が異なる。

【０１９１】すなわち、図２９のクーポン要求処理（Ｓ１２４００）の処理フローチャートは、図７に示したクーポン要求処理（Ｓ２４００）の処理フローチャートと同様であるが、販売者１００の公開鍵の代わりに発券者７００の公開鍵を用いる点と、暗号化したパスワード５０１の送信先が、販売者１００の代わりに発券者７００となる点とが異なる。

【０１９２】また、図２９のクーポン発券処理（Ｓ７３００）の処理フローチャートは、図８に示したクーポン発券処理（Ｓ１３００）の処理フローチャートと同様であるが、本処理を発券者７００が行う点（本処理がクーポン発券・検証処理プログラム７０７ｂによって実現される点）と、販売者１００の秘密鍵の代わりに発券者７００の秘密鍵を用いる点とが異なる。

【０１９３】また、図２９のクーポン受信処理（Ｓ１２５００）の処理フローチャートは、図９に示したクーポン受信処理（Ｓ２５００）の処理フローチャートと同様である。

【０１９４】図３０は、既にクーポンの発券を受けている消費者２００が、通信網３００を介してクーポンを使用し、販売者６００が、クーポンを検証するまでの動作を説明するための図である。

【０１９５】図３０において、既にクーポンの発券を受けている消費者２００は、クーポン使用オンライン処理（Ｓ２６００）を行い、クーポン受信処理（Ｓ１２５００）で入手したクーポン５０２と、暗号化した自身のパスワード５０１とを、販売者６００に対して送信する。

【０１９６】販売者６００は、クーポン５０２およびパスワード５０１を受信すると、後述するクーポン検証処理（Ｓ６４００）を行い、受信したクーポン５０２を検証する。

【０１９７】図３１は、既にクーポンの発券を受けている消費者２００が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者６００が、クーポンを検証するまでの動作を説明するための図である。

【０１９８】図３１において、既にクーポンの発券を受けている消費者２００は、クーポン使用オフライン処理（Ｓ２７００）を行い、印刷されたクーポン５０４を販売店に持参する。

【０１９９】販売者６００は、消費者２００が持参したクーポン５０４を受け取ると、後述するクーポン検証処理（Ｓ６４００）を行い、受け取ったクーポン５０４を検証する。

【０２００】図３０および図３１に示した動作は、各々、図５および図６に示した動作において、販売者６００が行うクーポン検証処理（Ｓ６４００）の処理内容のみが異なり、本処理の処理内容については後述する。

【０２０１】すなわち、図３０のクーポン使用オンライン処理（Ｓ２６００）の処理フローチャートは、図１０に示したクーポン使用オンライン処理（Ｓ２６００）の処理フローチャートと同様である。

【０２０２】また、図３１のクーポン使用オフライン処理（Ｓ２７００）の処理フローチャートは、図１１に示したクーポン使用オフライン処理（Ｓ２７００）の処理フローチャートと同様である。

【０２０３】図３２は、図３０および図３１のクーポン検証処理（Ｓ６４００）の処理フローチャートであり、本処理は、クーポン検証処理プログラム６０７ｂによって実現される。

【０２０４】図３２に示すように、クーポン検証処理（Ｓ６４００）においては、販売者６００は、図１２に示したクーポン検証処理（Ｓ１２００）と同様の処理を行うが、ステップ１１４０４の書面検証処理の処理内容が、後述するように異なる。

【０２０５】また、販売者６００は、使用済みシリアル番号リストを管理せず、ステップ１１４０６で、クーポンに記載されているシリアル番号を発券者７００に対して通知し、使用済みシリアル番号リストへのシリアル番号の登録を発券者７００に行ってもらうようにしている点が異なる。

【０２０６】図３３は、図３２の書面検証処理（ステップ１１４０４）の処理フローチャートである。

【０２０７】図３３に示すように、書面検証処理（ステップ１１４０４）においては、販売者６００は、図１３に示した書面検証処理と同様の処理を行うが、ステップ１１４１０で、クーポンに記載されているデジタル署名を、発券者７００の公開鍵を用いて復号している点と、ステップ１１４１４で、クーポンに記載されているシリアル番号を発券者７００に対して通知し、使用済みシリアル番号リストにシリアル番号が登録されているか否かを発券者７００に問い合わせるようにしている点とが異なる。そこで、販売者６００は、ステップ１４１１の検証では、ステップ１１４１０で復号した結果と、クーポンに記載されているクーポン情報とを比較することとなる。

【０２０８】以上説明したように、第３の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態と同様に、シリアル番号，有効期限，金額等の改ざんされては困るクーポン情報のデジタル署名を、発券者７００だけしか知らない情報である秘密鍵を用いて計算し、計算したデジタル署名を、目視可能なデータとして記載したクーポンを作成するようにしている。

【０２０９】従って、第３の実施形態に係る電子クーポンシステムによれば、上述した第１の実施形態と同様に、消費者２００が電子的なクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されているデジタル署名を検証することで、クーポンの偽造や改ざんを検出することができる。

【０２１０】なお、第３の実施形態に係る電子クーポンシステムでは、デジタル署名を作成する発券者７００と、デジタル署名を検証する販売者６００とが異なるが、デジタル署名の作成時に発券者７００の秘密鍵を用い、デジタル署名の検証時に発券者７００の公開鍵を用いるようにすることで、販売者６００によるデジタル署名の検証が可能である。ただし、販売者６００および発券者７００の双方だけしか知らない秘密の暗号鍵を用いて、クーポン情報を暗号化し、暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにしても、販売者６００による暗号化情報の検証は可能である。

【０２１１】また、第３の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態と同様に、クーポンの発券時に、消費者２００が提示したパスワードの不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしている。さらに、クーポンの使用時には、発券を要求した消費者２００だけしか知らないパスワードを販売者６００に提示し、消費者２００が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較するようにしている。

【０２１２】従って、第３の実施形態に係る電子クーポンシステムによれば、上述した第１の実施形態と同様に、たとえクーポンが盗まれたとしても、クーポンの発券要求時に提示されたパスワードを知らない第三者がクーポンを不正使用するのを防止することができる。

【０２１３】なお、第３の実施形態に係る電子クーポンシステムにおいては、パスワードについて、不可逆変換を施した不可逆変換値を、目視可能なデータとしてクーポンに記載するようにした例を示しており、本例によれば、不可逆変換方法を公開しても支障がないので、販売者６００による不可逆変換値の検証が可能であると共に、パスワードの不可逆変換値が不一致である場合に、消費者２００が、自身が提示したパスワードの不可逆変換値を計算して確認することが可能である。しかしながら、パスワードについて、販売者６００および発券者７００の双方だけしか暗号化できない暗号化方法で暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにしても、販売者６００による暗号化情報の検証は可能である。

【０２１４】なお、第３の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【０２１５】例えば、第３の実施形態に係る電子クーポンシステムにおいては、消費者２００は、発券者７００および販売者６００に対してパスワードを送信するときに、発券者７００および販売者６００の公開鍵を取得し、暗号通信を行うようにしているが、本発明はこれに限定しない。消費者２００は、１度、発券者７００および販売者６００の公開鍵を入手すれば、２回以降は、その公開鍵を使うことができる。また、発券者７００および販売者６００と消費者２００との間で共通の鍵を持つことができれば、秘密鍵暗号技術を使って暗号化するようにしてもよい。

【０２１６】また、第３の実施形態に係る電子クーポンシステムにおいて、消費者２００から発券者７００および販売者６００に対してパスワードを送信するときに、暗号化されたパスワードがそのまま盗まれて不正使用されるのを防止するために、パスワードを、その他の情報（乱数や適当な数字でよい。）と共に暗号化して送信するようにしてもよい。

【０２１７】また、第３の実施形態に係る電子クーポンシステムにおいては、発券者７００は、デジタル署名を、数値や文字等の目視可能なデータとしてクーポンに記載するようにしているが、印刷後に目視可能であれば、例えば、バーコード等のようなものであってもよい。バーコードとして記載すれば、販売者６００は、印刷されたクーポンから各種情報を取得する際に、バーコードリーダを用いることができるようになる。

【０２１８】また、第３の実施形態に係る電子クーポンシステムにおいては、発券者７００は、消費者２００のパスワードの不可逆変換値と、シリアル番号，有効期

限，金額等のクーポン情報のデジタル署名とを、別々にクーポンに記載するようにしているが、クーポン情報と共に、パスワードも一緒にデジタル署名を計算するようにしてもよい。また、このとき、クーポン情報やパスワード等の、デジタル署名を計算する元の情報は、不可逆変換を施した後に、デジタル署名を計算するようにしてもよい。

【０２１９】また、第３の実施形態に係る電子クーポンシステムにおいては、消費者２００から使用が要求されたクーポンを販売者６００が検証し、クーポンの二重使用のみを発券者７００が一元管理して検証する方法を取っているが、販売者６００が受け取ったクーポンを、そのときに提示されたパスワードと共に発券者７００に提示し、発券者７００側でクーポンを検証するようにしてもよい。また、その両方を組み合わせるようにしてもよい。

【０２２０】発券者７００側でクーポンを検証するようにすれば、発券者７００だけしか知らない秘密の暗号鍵を用いてクーポン情報を暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにすることができる。また、発券者７００だけしか暗号化できない暗号化方法でパスワードを暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにすることもできる。

【０２２１】（第４の実施形態）ところで、上述した第３の実施形態に係る電子クーポンシステムにおいて、発券者７００は、上述した第２の実施形態で説明したように、チケットを取り扱うようにすることができ、そのようにした場合を、第４の実施形態として、上述した第２の実施形態および第３の実施形態と異なる点についてのみ説明する。

【０２２２】第４の実施形態に係る電子クーポンシステムの概略構成は、図２６に示した概略構成と同様である。

【０２２３】図３４は発券者端末７０１のハードウェア構成を示す図である。

【０２２４】図２７に示したハードウェア構成と異なる点は、メモリ７０７に、チケット発券・検証処理プログラム７０７ｃが一時的に格納される点である。

【０２２５】チケット発券・検証処理プログラム７０７ｃは、消費者２００に対してチケットを発券したり、消費者２００から使用が要求されたチケットを検証したりするためのプログラムである。

【０２２６】なお、販売者端末６０１のハードウェア構成は、図２８に示したハードウェア構成と同様であり、消費者端末２０１のハードウェア構成は、図１６に示したハードウェア構成と同様である。

【０２２７】次に、第４の実施形態に係る電子クーポンシステムの動作について説明する。

【０２２８】なお、以下の説明おいても、上述した第３の実施形態と同様に、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、発券者７００が行う処理は、実際には、発券者７００の指示によって発券者端末７０１が実行するものである。

【０２２９】図３５は、消費者２００が、発券者７００に対して１枚目のチケットの発券を要求し、発券者７００によって発券された１枚目のチケットを受信するまでの動作を説明するための図である。なお、チケットは、ｎ枚だけ集めたときに効力を発揮するものとする。

【０２３０】図３５において、まず、消費者２００は、後述する初期チケット発券要求処理（Ｓ１２１００）を行い、暗号化した自身のパスワード５０１を、発券者７００に対して送信する。

【０２３１】発券者７００は、パスワード５０１を受信すると、後述する初期チケット発券処理（Ｓ７１００）を行い、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）５０５と、受信したパスワード５０１，ＵＩＤ５０５，発券者７００だけしか知らない秘密の情報（例えば、発券者７００の秘密鍵）を連結したものの、ｎ番目の不可逆変換値H_n（506_n）とを、１枚目のチケットとして、消費者２００に対して送信する。

【０２３２】消費者２００は、ＵＩＤ５０５およびH_n（506_n）を受信すると、後述するチケット受信処理（Ｓ１２２００）を行い、受信したＵＩＤ５０５およびH_n（506_n）を保管する。

【０２３３】図３５に示した動作は、図１７に示した動作において、販売者１００が発券者７００に代わっている点が異なる。

【０２３４】すなわち、図３５の初期チケット発券要求処理（Ｓ１２１００）の処理フローチャートは、図１９に示した初期チケット発券要求処理（Ｓ２１００）の処理フローチャートと同様であるが、販売者１００の公開鍵の代わりに発券者７００の公開鍵を用いる点と、暗号化したパスワード５０１の送信先が、販売者１００の代わりに発券者７００となる点とが異なる。

【０２３５】また、図３５の初期チケット発券処理（Ｓ７１００）の処理フローチャートは、図２０に示した初期チケット発券処理（Ｓ１１００）の処理フローチャートと同様であるが、本処理を発券者７００が行う点（本処理がチケット発券・検証処理プログラム７０７ｃによって実現される点）と、販売者１００の秘密鍵の代わりに発券者７００の秘密鍵を用いる点とが異なる。

【０２３６】また、図３５のチケット受信処理（Ｓ１２２００）の処理フローチャートは、図２１に示したチケット受信処理（Ｓ２２００）の処理フローチャートと同様である。

【０２３７】図３６は、消費者２００が、発券者７００

に対して２枚目以降のチケットの発券を要求し、発券者７００によって発券された２枚目以降のチケットを受信するまでの動作を説明するための図である。

【０２３８】図３６において、まず、消費者２００は、２枚目のチケットの発券を受ける場合は、後述するチケット発券要求処理（Ｓ１２３００）を行い、暗号化した自身のパスワード５０１と、１枚目のチケット受信処理（Ｓ１２２００）で入手したＵＩＤ５０５およびH_n（506_n）とを、発券者７００に対して送信する。

【０２３９】発券者７００は、パスワード５０１，ＵＩＤ５０５，H_n（506_n）を受信すると、後述するチケット発券処理（Ｓ７２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，H_n（506_n）と、発券者７００の秘密鍵とから、H_{n-1}（506_{n-1}）を求めて、求めたH_{n-1}（506_{n-1}）を、２枚目のチケットとして、消費者２００に対して送信する。

【０２４０】消費者２００は、H_{n-1}（506_{n-1}）を受信すると、チケット受信処理（Ｓ１２２２００）を行い、受信したH_{n-1}（506_{n-1}）を保管する。

【０２４１】同様に、消費者２００は、ｍ＋１枚目（１≦ｍ＜ｎ）のチケットの発券を受ける場合は、チケット発券要求処理（Ｓ１２３００）を行い、暗号化した自身のパスワード５０１と、ｍ枚目のチケット受信処理（Ｓ１２２００）で入手したＵＩＤ５０５および$H_{n-(m-1)}$（$506_{n-(m-1)}$）とを、発券者７００に対して送信する。

【０２４２】発券者７００は、パスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}$（$506_{n-(m-1)}$）を受信すると、チケット発券処理（Ｓ７２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}$（$506_{n-(m-1)}$）と、発券者７００の秘密鍵とから、H_{n-m}（506_{n-m}）を求めて、求めたH_{n-m}（506_{n-m}）を、ｍ＋１枚目のチケットとして、消費者２００に対して送信する。

【０２４３】消費者２００は、H_{n-m}（506_{n-m}）を受信すると、チケット受信処理（Ｓ１２２２００）を行い、受信したH_{n-m}（506_{n-m}）を保管する。

【０２４４】このようにして、消費者２００は、ｎ枚のチケットを集めることができ、これらｎ枚のチケットの効力を発揮させたい場合には、チケット発券要求処理（Ｓ１２３００）を行い、暗号化された自身のパスワード５０１と、ｎ枚目のチケット受信処理（Ｓ１２２００）で入手したＵＩＤ５０５およびH_1（506_1）とを、発券者７００に対して送信する。

【０２４５】発券者７００は、パスワード５０１，ＵＩＤ５０５，H_1（506_1）を受信すると、チケット発券処理（Ｓ７２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，H_1（506_1）と、発券者７００の秘密鍵とから、消費者２００がｎ枚だけチケットを集めたことを確認し、ｎ枚のチケット収集終了処理（Ｓ７２５０）を行う。

【０２４６】図３６に示した動作は、図１８に示した動作において、販売者１００が発券者７００に代わっている点が異なる。

【０２４７】すなわち、図３６のチケット発券要求処理（Ｓ１２１００）の処理フローチャートは、図２２に示したチケット発券要求処理（Ｓ２３００）の処理フローチャートと同様であるが、販売者１００の公開鍵の代わりに発券者７００の公開鍵を用いる点と、暗号化したパスワード５０１，保存しているＵＩＤ５０５およびH_mの送信先が、販売者１００の代わりに発券者７００となる点とが異なる。

【０２４８】また、図３６のチケット発券処理（Ｓ７１００）の処理フローチャートは、図２３に示したチケット発券処理（Ｓ１２００）の処理フローチャートと同様であるが、本処理を発券者７００が行う点（本処理がチケット発券・検証処理プログラム７０７ｃによって実現される点）と、販売者１００の秘密鍵の代わりに発券者７００の秘密鍵を用いる点とが異なる。

【０２４９】また、図３６のチケット受信処理（Ｓ１２２００）の処理フローチャートは、図２１に示したチケット受信処理（Ｓ２２００）の処理フローチャートと同様である。

【０２５０】なお、チケットをｎ枚だけ集めたときに発揮する効力は、販売者１００の販売方針に応じて異なるようにすることができるが、チケットをｎ枚だけ集めたか否かの判定を、発券者７００が行うようにしているので、図３６のチケット収集終了処理（Ｓ７２５０）は、発券者７００が行うものとしている。

【０２５１】以上説明したように、第４の実施形態に係る電子クーポンシステムにおいても、上述した第２の実施形態と同様に、チケットの発券時に、発券者７００だけしか知らない秘密の情報である発券者７００の秘密鍵，消費者２００だけしか知らない情報であるパスワード，ｎ枚のチケットの組を識別するためのＵＩＤを連結したものから、不可逆変換値を繰り返し計算し、ｎ番目の不可逆変換値H_n，ｎ－１番目の不可逆変換値H_{n-1}，…，２番目の不可逆変換値H_2，１番目の不可逆変換値H_1という順番で、各不可逆変換値を消費者２００に対して返信するようにしている。また、消費者２００から発券者７００に対して、１回前に送信されたH_m，ＵＩＤ，パスワードを送信するようにしている。また、不可逆変換値を計算するのに必要な消費者２００ごとのデータは、消費者２００から発券者７００に対して送信されるようにしている。

【０２５２】従って、第４の実施形態に係る電子クーポンシステムによれば、上述した第３の実施形態による効果に加えて、上述した第２の実施形態と同様に、たとえチケットが通信路上で盗まれたとしても、パスワードを知らない第三者がチケットを不正使用するのを防止することができると共に、発券者７００側で、消費者２００

ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【０２５３】なお、第４の実施形態に係る電子クーポンシステムにおいても、上述した第３の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【０２５４】例えば、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、発券者７００の秘密鍵を用いて不可逆変換値を計算するようにしているが、この計算は、発券者７００以外が計算不可能であればよいので、不可逆変換のアルゴリズムが非公開であれば、発券者７００の秘密鍵を用いなくてもよい。

【０２５５】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００が、初期チケット発券時に、消費者２００に対してＵＩＤを送信し、消費者２００が、そのＵＩＤを保管しておき、その後は、保管しておいたＵＩＤを消費者２００から発券者７００に対して送信するようにしているが、チケット発券時に、その都度、発券者７００から消費者２００に対してＵＩＤを送信するようにしてもよい。

【０２５６】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、発券者７００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワードおよびＵＩＤを連結したものを、発券者７００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における発券者７００の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者２００に対して返信するようにしてもよい。詳しくは、発券者７００は、パスワードおよびＵＩＤを連結したものの暗号化情報H_1に基づいて、暗号化情報H_i（$1 \leqq i < n$）の暗号化情報H_{i+1}を順次計算し、ｎ番目の暗号化情報H_n，ｎ－１番目の暗号化情報H_{n-1}，…，２番目の暗号化情報H_2，１番目の暗号化情報H_1という順番で、各暗号化情報を消費者２００に対して返信するようにしてもよい。

【０２５７】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、発券者７００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワード，ＵＩＤ，何枚目のチケットであるかを示す枚数情報を連結したものを、発券者７００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における発券者７００の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者２００に対して返信するようにしてもよい。このようにすれば、発券者７００は、消費者２００からチケットの発券要求時に送信されてくる暗号化情報を、発券者７００だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報によって、消費者２００が何枚のチケットを集めたかを知ることができる。

【０２５８】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、不可逆変換値を消費者２００に対して送信するようにしているが、上述した第１の実施形態で説明したクーポンと同様に、不可逆変換値を目視可能なデータとして記載したチケットを作成し、書面としてのチケットを消費者２００に対して送信するようにしてもよい。

【０２５９】さらに、第４の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したクーポンと同様に、発券者７００から消費者２００に対して、チケットと共に、チケット全体のデジタル署名が送信されるようにしてもよく、このようにすれば、チケットの発券を受けた消費者２００側で、受け取ったチケットが改ざんされていないか否かを検証することができる。

【０２６０】

【発明の効果】以上説明したように、本発明によれば、電子的に発券されたクーポンが印刷されて使用される場合でも、クーポンの偽造や改ざん，第三者によるクーポンの不正使用を検出することができるようになるので、消費者は、電子的に発券されたクーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようになる。

【０２６１】さらに、本発明によれば、複数枚だけ集めたときに効力を発揮するチケットを取り扱う場合に、チケットを発券する側で消費者を管理する必要がなくなるので、チケットを発券する側の手間を減らすことができるようになる。

【図面の簡単な説明】

【図１】第１の実施形態に係る電子クーポンシステムの概略構成図。

【図２】第１の実施形態における販売者端末のハードウェア構成図。

【図３】第１の実施形態における消費者端末のハードウェア構成図。

【図４】第１の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対してクーポンの発券を要求し、販売者によって発券されたクーポンを受信するまでの動作の説明図。

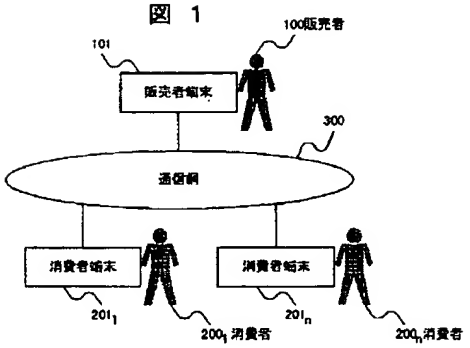
【図５】第１の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、通信網を介してクーポンを使用し、販売者が、クーポンを検証するまでの動作の説明図。

【図６】第１の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者が、クーポンを検証するまでの

動作の説明図。
【図７】図４のクーポン要求処理の処理フローチャート。
【図８】図４のクーポン発券処理の処理フローチャート。
【図９】図４のクーポン受信処理の処理フローチャート。
【図１０】図５のクーポン使用オンライン処理の処理フローチャート。
【図１１】図６のクーポン使用オフライン処理の処理フローチャート。
【図１２】図５および図６のクーポン検証処理の処理フローチャート。
【図１３】図１２のステップ１４０４で行われる書面検証処理の処理フローチャート。
【図１４】第１の実施形態に係る電子クーポンシステムで発券されるクーポンの形式の一例を示す説明図。
【図１５】第２の実施形態における販売者端末のハードウェア構成図。
【図１６】第２の実施形態における消費者端末のハードウェア構成図。
【図１７】第２の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対して１枚目のチケットの発券を要求し、販売者によって発券された１枚目のチケットを受信するまでの動作の説明図。
【図１８】第２の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対して２枚目以降のチケットの発券を要求し、販売者によって発券された２枚目以降のチケットを受信するまでの動作の説明図。
【図１９】図１７の初期チケット発券要求処理の処理フローチャート。
【図２０】図１７の初期チケット発券処理の処理フローチャート。
【図２１】図１７および図１８のチケット受信処理の処理フローチャート。
【図２２】図１８のチケット発券要求処理の処理フローチャート。
【図２３】図１８のチケット発券処理の処理フローチャート。
【図２４】図２０のステップ１１０５で不可逆変換値が計算される様子を示す説明図。
【図２５】第２の実施形態における消費者端末での表示の一例を示す説明図。
【図２６】第３の実施形態に係る電子クーポンシステムの概略構成図。
【図２７】第３の実施形態における発券者端末のハードウェア構成図。
【図２８】第３の実施形態における販売者端末のハードウェア構成図。
【図２９】第３の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対してクーポンの発券を要求し、発券者によって発券されたクーポンを受信するまでの動作の説明図。
【図３０】第３の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、通信網を介してクーポンを使用し、販売者が、クーポンを検証するまでの動作の説明図。
【図３１】第３の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者が、クーポンを検証するまでの動作の説明図。
【図３２】図３０および図３１のクーポン検証処理の処理フローチャート。
【図３３】図３２のステップ１１４０４で行われる書面検証処理の処理フローチャート。
【図３４】第４の実施形態における発券者端末のハードウェア構成図。
【図３５】第４の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対して１枚目のチケットの発券を要求し、発券者によって発券された１枚目のチケットを受信するまでの動作の説明図。
【図３６】第４の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対して２枚目以降のチケットの発券を要求し、発券者によって発券された２枚目以降のチケットを受信するまでの動作の説明図。
【符号の説明】
１００，６００…販売者、200_1～200_n…消費者、７００…発券者、１０１，601_1～601_n…販売者端末、201_1～201_n…消費者端末、７０１…発券者端末、３００…通信網、１０２，２０２，７０２…通信網インタフェース、１０３，２０３，７０３…表示装置、１０４，２０４，７０４…入力装置、１０５，２０５，７０５…記憶装置、１０６，２０６，７０６…中央処理装置（ＣＰＵ）、１０７，２０７，７０７…一時記憶装置（メモリ）、２０８…印刷装置、１１０，２１０，７１０…バス、１０７ａ，２０７ａ，７０７ａ…オペレーティングシステム（ＯＳ）、１０７ｂ，７０７ｂ…クーポン発券・検証処理プログラム、１０７ｃ，７０７ｃ…チケット発券・検証処理プログラム、２０７ｂ…クーポン要求・受信・発信処理プログラム、６０７ｂ…クーポン検証処理プログラム、２０７ｃ…チケット要求・受信・発信処理プログラム、５０１…パスワード、５０２…クーポン、５０３…デジタル署名、５０４…印刷されたクーポン、５０５…ＵＩＤ、506_1～506_n…不可逆変換値、５０７…秘密鍵。

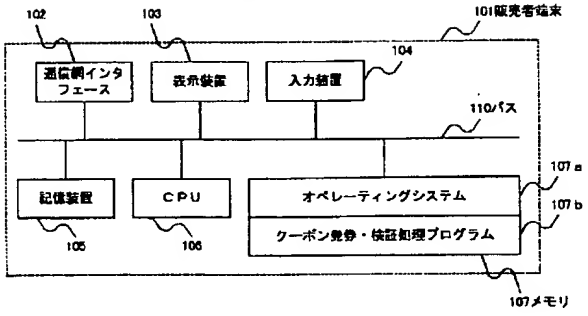
【図１】

図 1



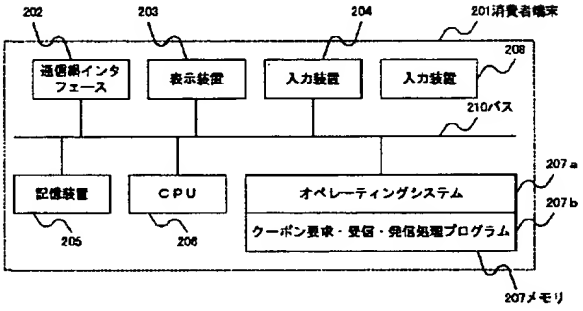
【図２】

図 2



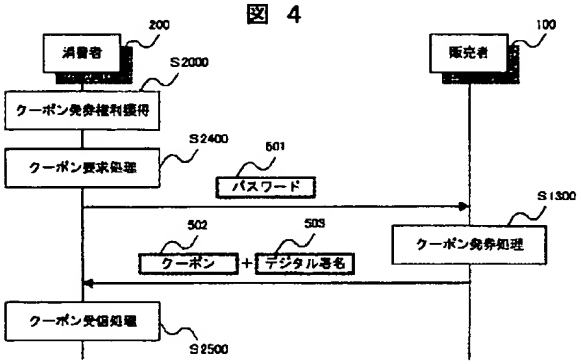
【図３】

図 3



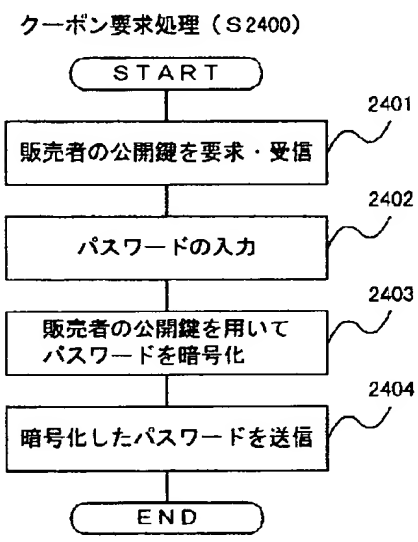
【図４】

図 4



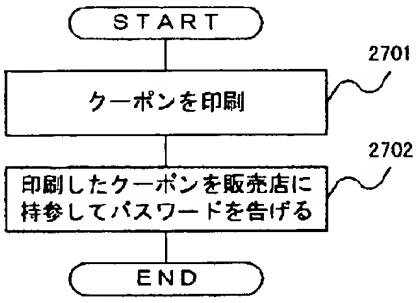
【図７】

図 7



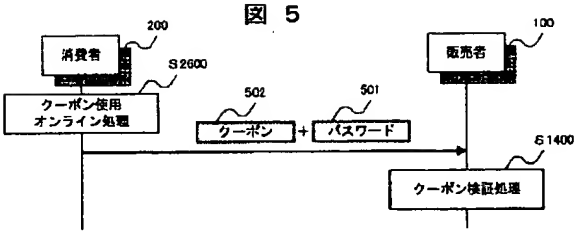
【図１１】

図 11



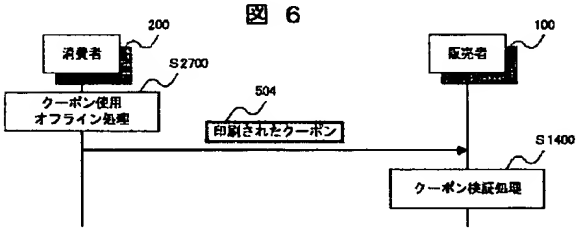
【図５】

図 5



【図６】

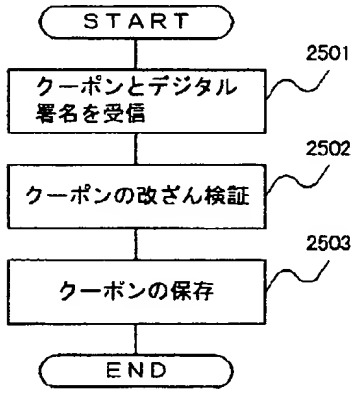
図 6



【図９】

図 9

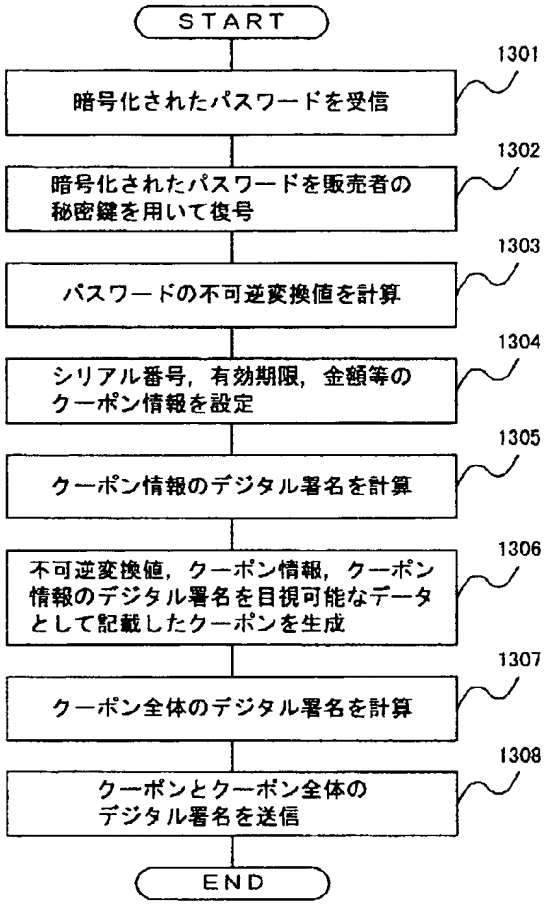
クーポン受信処理（S2500）



【図８】

図 8

クーポン発券処理（S1300）



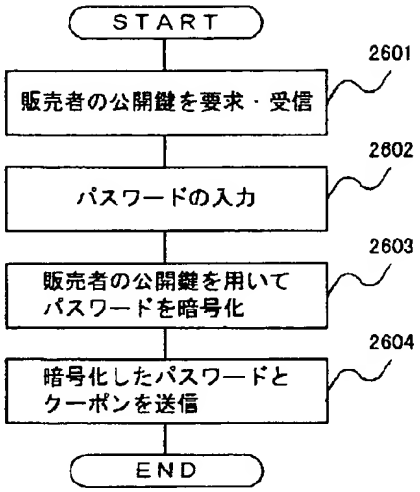
【図１４】

図 14

【図１０】

図 10

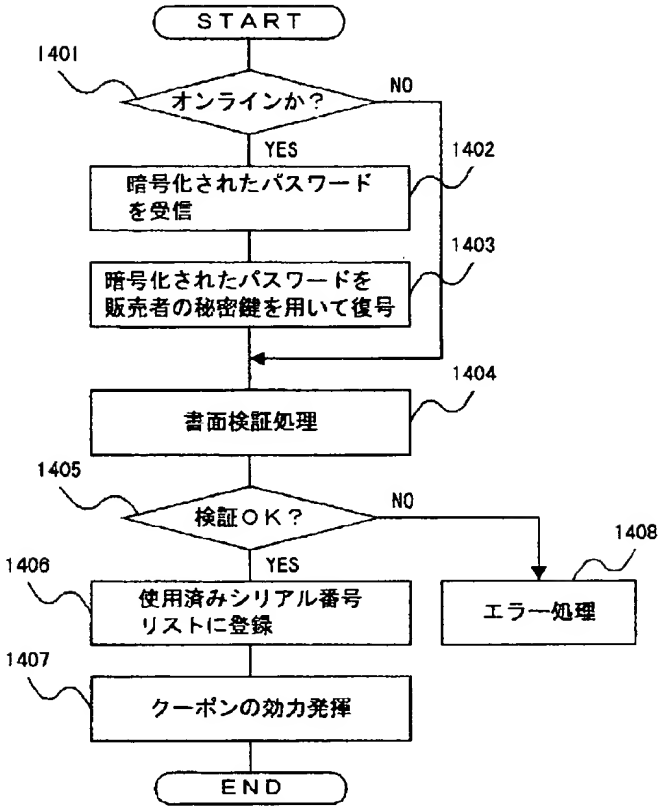
クーポン使用オンライン処理（Ｓ2600）



【図１２】

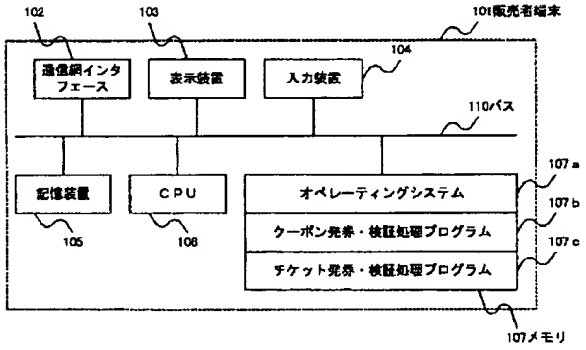
図 12

クーポン検証処理（Ｓ1400）



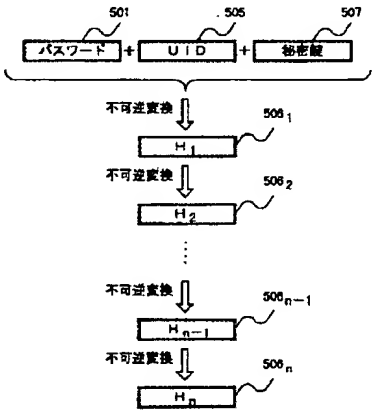
【図１５】

図 15



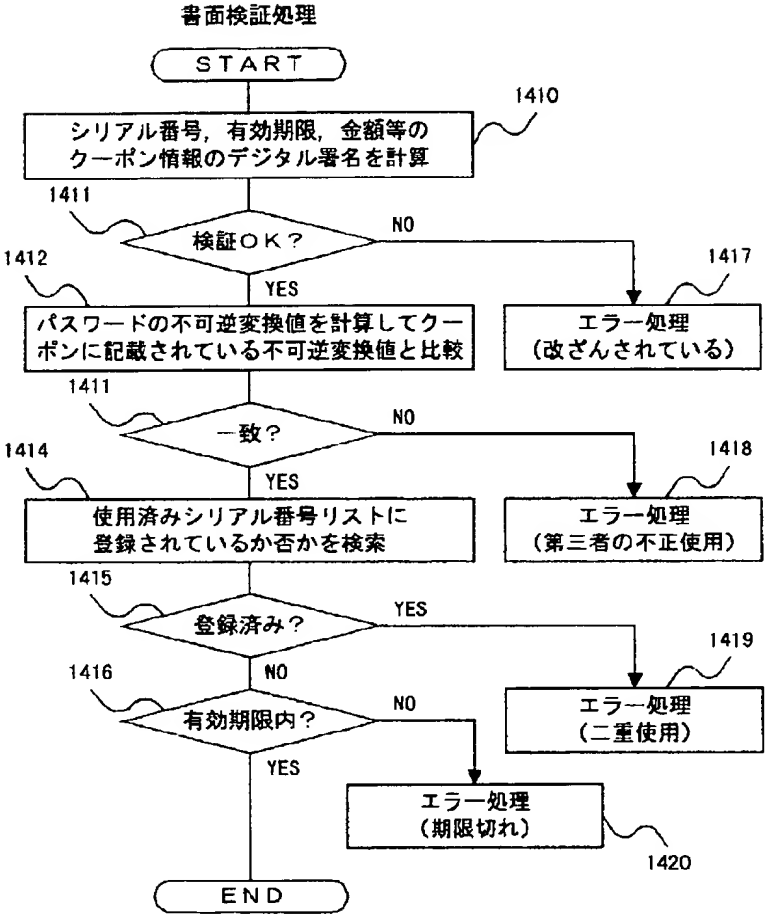
【図２４】

図 24



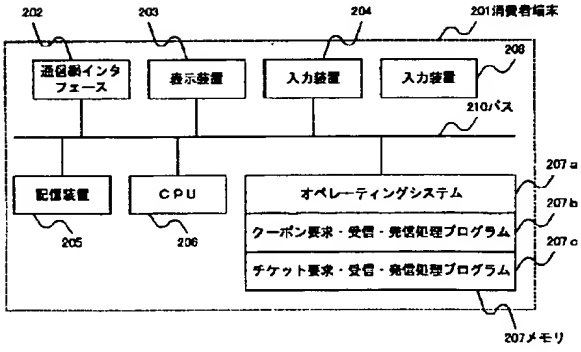
【図１３】

図 13



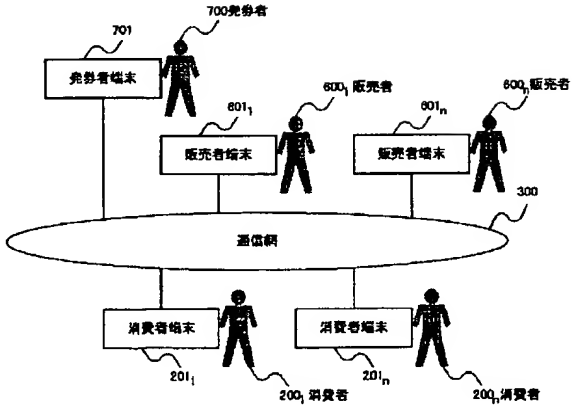
【図１６】

図 16



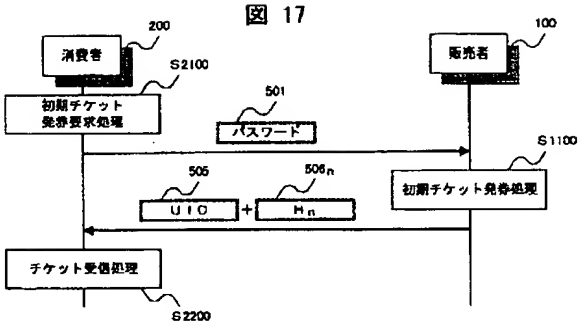
【図２６】

図 26



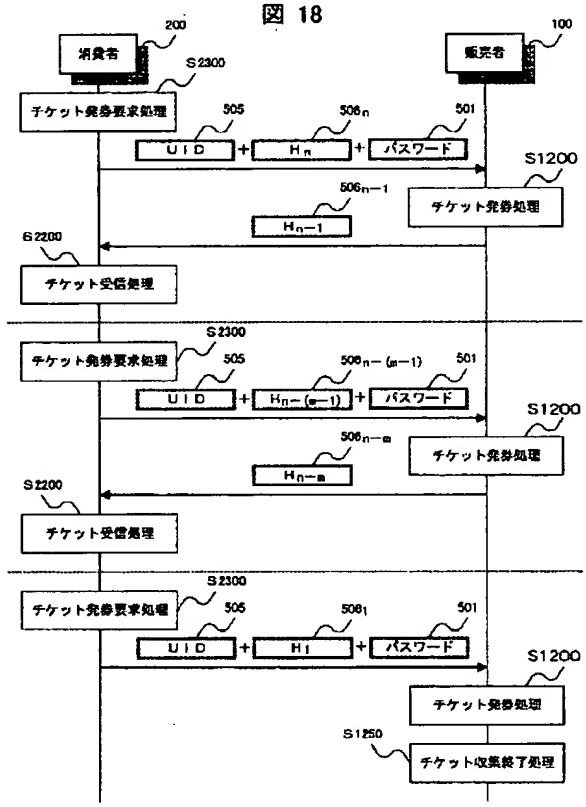
【図１７】

図 17



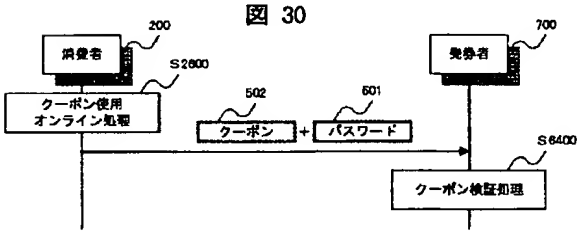
【図１８】

図 18



【図３０】

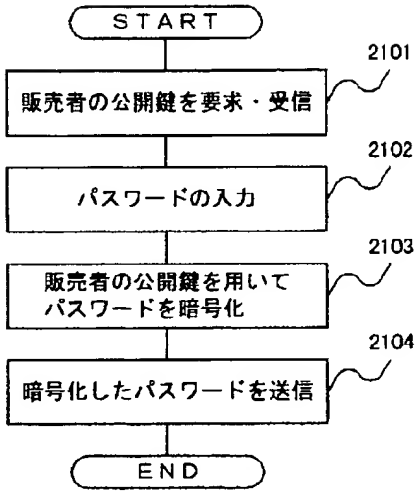
図 30



【図１９】

図 19

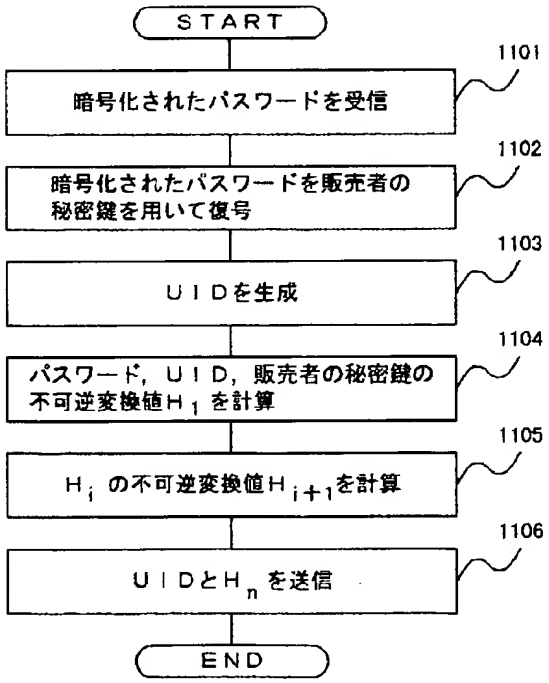
初期チケット発券要求処理（S2100）



【図２０】

図 20

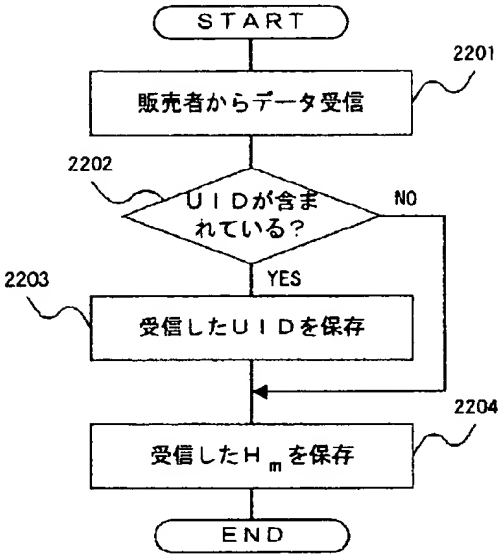
初期チケット発券処理（S1100）



【図２１】

図 21

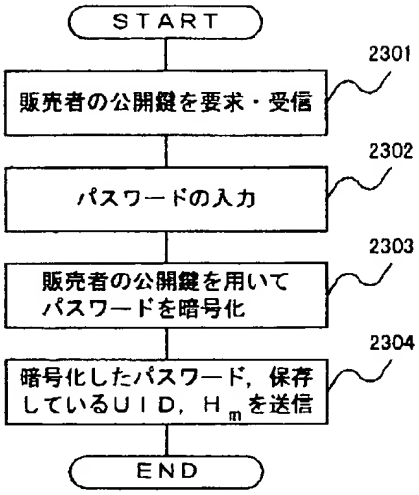
チケット受信処理（Ｓ2200）



【図２２】

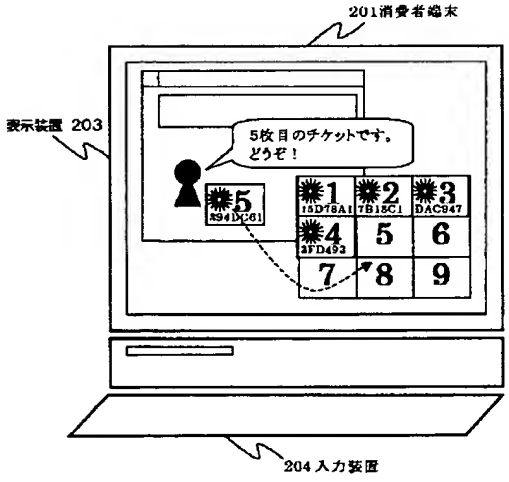
図 22

チケット発券要求処理（Ｓ2300）



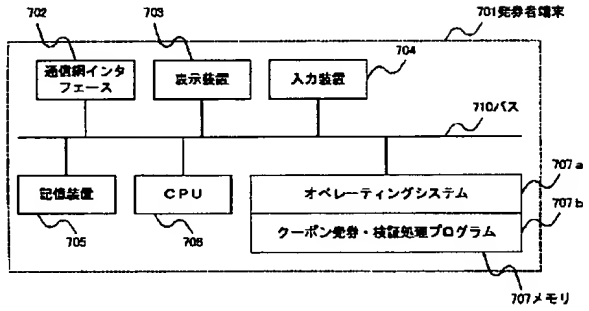
【図２５】

図 25



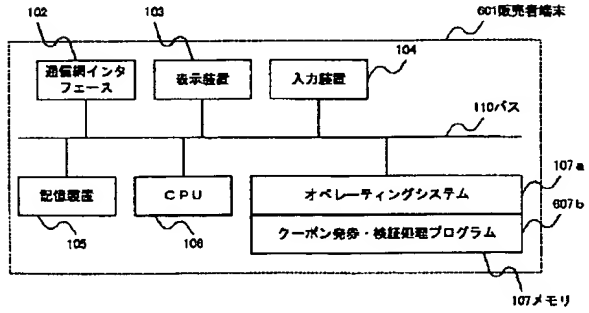
【図２７】

図 27



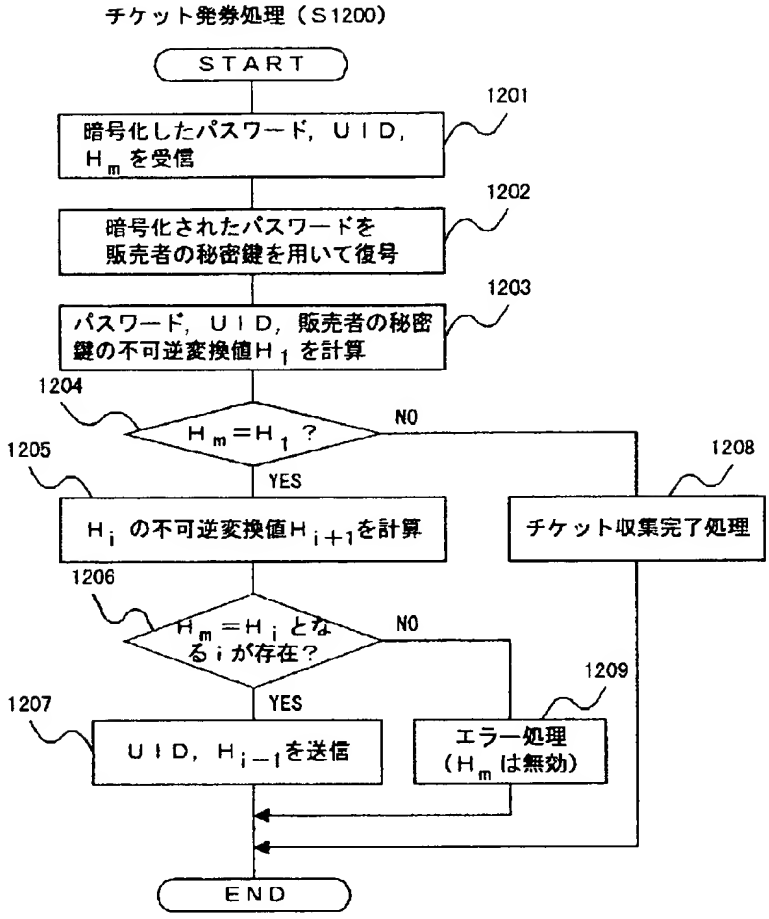
【図２８】

図 28



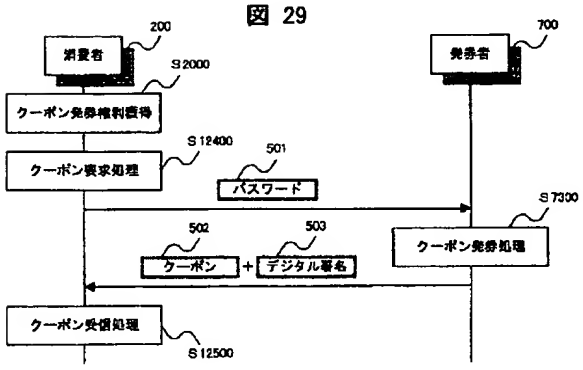
【図２３】

図 23



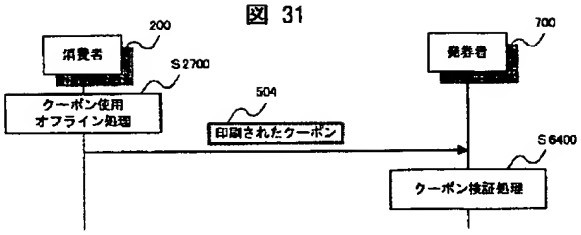
【図２９】

図 29



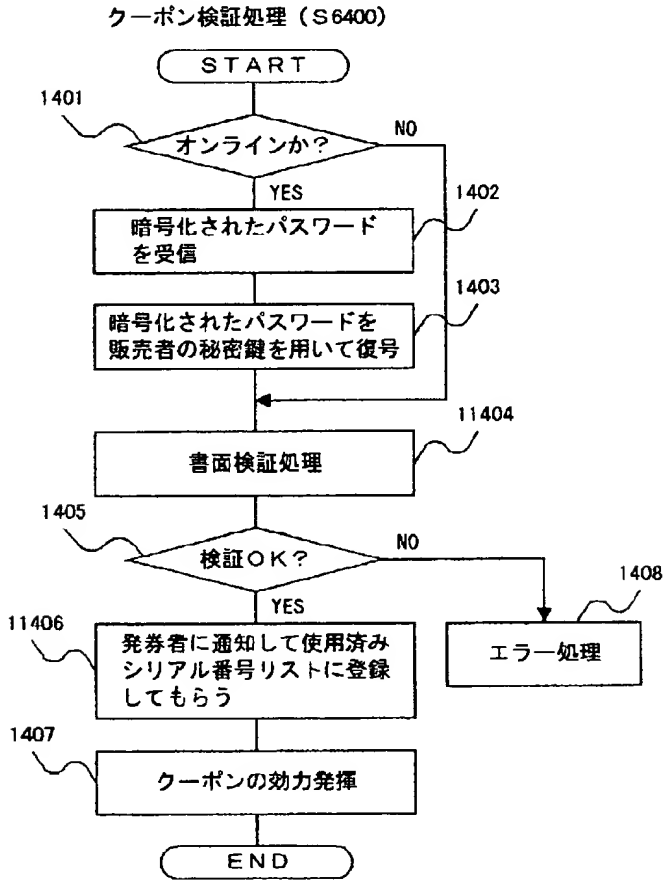
【図３１】

図 31



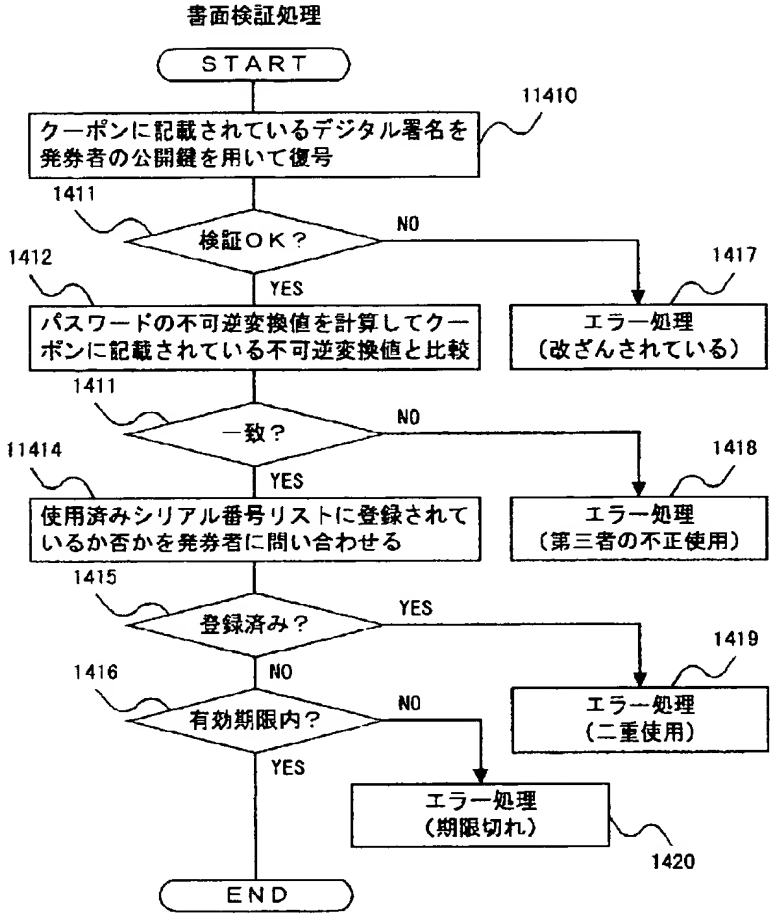
【図３２】

図 32



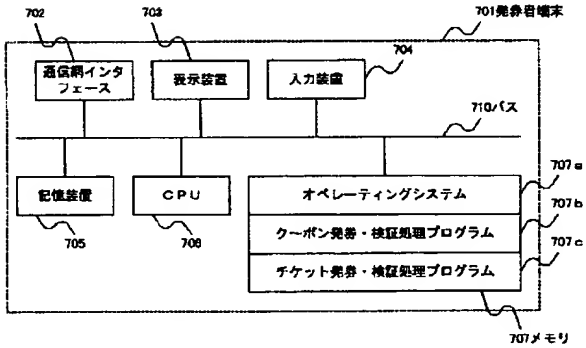
【図３３】

図 33



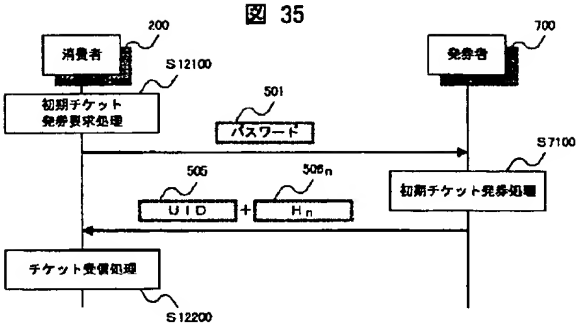
【図３４】

図 34



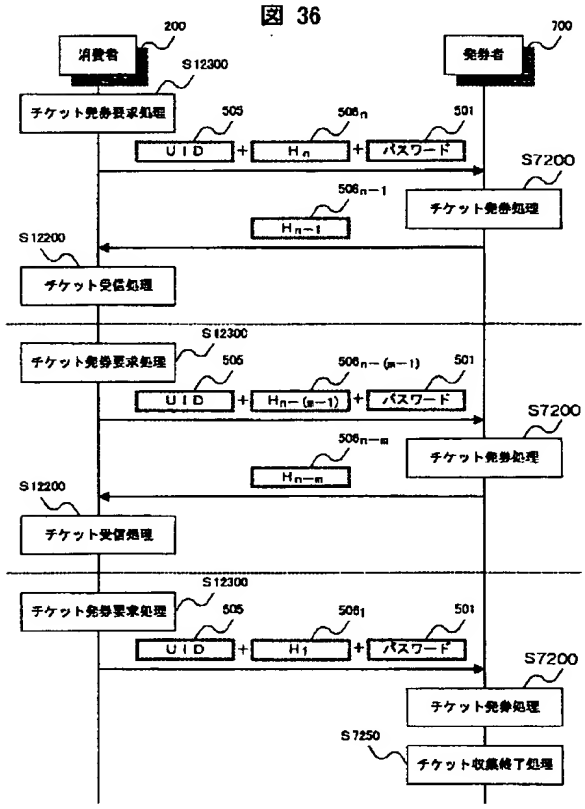
【図３５】

図 35



【図３６】

図 36



フロントページの続き

(72)発明者　豊島　久
東京都江島区新砂一丁目６番27号　株式会
社日立製作所公共情報事業部内

(72)発明者　齋藤　司
東京都江島区新砂一丁目６番27号　株式会
社日立製作所公共情報事業部内